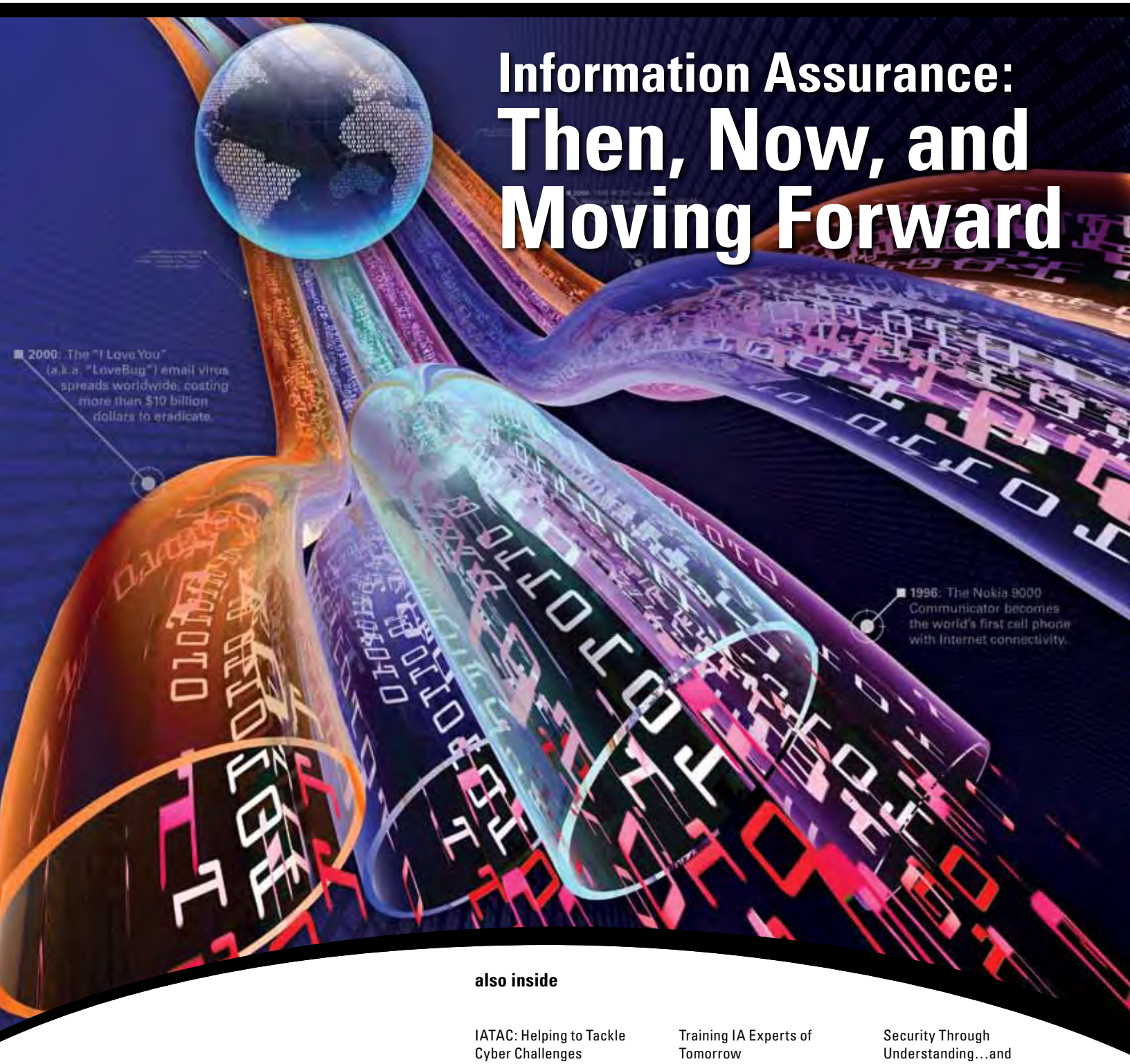
15/1

Volume 15 Number 1 • **Winter 2012**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals



Information Assurance: Then, Now, and Moving Forward

also inside

IATAC

contents

About IATAC and the *IAnewsletter*
The *IAnewsletter* is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), and Assistant Secretary of Defense for Research & Engineering ASD(R&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the US Government, DoD, DTIC, or ASD(R&E). The mention of commercial products does not imply endorsement by DoD or ASD(R&E).

Inquiries about IATAC capabilities, products, and services may be addressed to—

IATAC Director: Gene Tyler
Inquiry Services: Karen Goertzel

If you are interested in contacting an author directly, please e-mail us at *iatac@dtic.mil*.

***IAnewsletter* Staff**
Chief Editor: Gene Tyler
Assistant Editor: Kristin Evans
Art Director: Tammy Black
Copy Editor: Alexandra Sveum
Editorial Board: Al Arnold, Angela Orebaugh, Dr. Ronald Ritchey
Designer: Tammy Black

***IAnewsletter* Article Submissions**
To submit your articles, notices, programs, or ideas for future issues, please visit *http://iac.dtic.mil/iatac/IA_newsletter.html* and download an "Article Instructions" packet.

***IAnewsletter* Address Changes/ Additions/Deletions**
To change, add, or delete your mailing or e-mail address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
13200 Woodland Park Road
Suite 6031
Herndon, VA 20171

Phone: 703/984-0775
Fax: 703/984-0773

E-mail: *iatac@dtic.mil*
URL: *http://iac.dtic.mil/iatac*

Cover design: Dustin Hurt
Centerfold design: Donald Rowe
Newsletter design: Donald Rowe

Distribution Statement A: Approved for public release; distribution is unlimited.

in every issue

IATAC Chat

Gene Tyler, IATAC Director

Well, this is a farewell that I have dreaded writing, and I have known it has been coming for some time. I have found every way possible to procrastinate—dental work without novocain, long protracted discussions with my mother-in-law, spring cleaning in the office (and it is winter, but you get the message)—discussing the Information Assurance Technology Analysis Center (IATAC) transition that is around the corner. Christopher Zember's article, "CSIAC Prepares Organizations to Tackle the Newest Battlespace- Cyberspace" addresses this transformation and how IATAC will become a part of the Cyber Security and Information Systems Information Analysis Center (CSIAC). Mr. Zember, Department of Defense Information Analysis Center leadership, and contracting officials are still working on the exact timeline and specifics about the transition, but change will happen soon. Ultimately, the *IAnewsletter* will change its name under CSIAC, and it may even become a virtual publication. If, for some reason, the transition is delayed, you could see one more edition of the *IAnewsletter* online. Regardless, this will be our last printed version of the *IAnewsletter*. We, in IATAC, fully support CSIAC and the changes that will take place soon. We are committed to making CISIAC a success!

So, we took this opportunity to build an *IAnewsletter* appropriate for a farewell edition. General Hernandez of Army Cyber Command contributes a super article that really addresses operationalizing information assurance (IA), a topic of great interest to the community. We have an interesting article by Dr. Victoria Victor about an Army and National Science Center project that focuses on cybersecurity for kids. Believe me, my 11-year-old granddaughter is already benefitting from this type of training at school. As a matter of fact, earlier this fall, she asked me if I knew anything about cybersecurity. Sure enough, she was working on a project similar to what Dr. Victor discusses. We also feature a great article by Rick Aldrich, our resident IA lawyer, on the linkage of IA with legal issues and world events. To go along with all of this edition's articles, our chief researcher and several others contributed to a timeline and history of IA—great information.

Things change, and as my old Army sergeant told me a long time ago, "Sir, if we ain't changin' then we ain't growin'"; and Winston Churchill said, "to improve is to change." We have made a number of significant changes over the past few years, and we fully support the upcoming CSIAC transition. This publication has become well respected in the IA community, and we have won numerous awards. Our readership has grown; the total distribution for the *IAnewsletter* exceeds 1.4 million copies, and throughout our growth, our leadership and team have stayed rock-solid. IATAC's first director and *IAnewsletter* publisher was Bob Thompson, who is still engaged with IATAC and is now a Principal at Booz Allen Hamilton. Our second director, who is also still engaged with IATAC, was Bob Lamb, now a Senior Vice President at Booz Allen.

As IATAC's last director, I get to work with the world's best team: Al Arnold, Christian Johnson, Peggy O'Connor, Kristin Evans, a world-class graphic design team, and many more. In addition, I have the good fortune of working with nearly 25,000 Booz Allen employees, all of whom are ready and willing to assist IATAC—all I have to do is ask. Additionally, we have had super government leadership; Terry Heston, Christopher Zember, Paul Repak, John Lower, Maria Green, and Sandy Schwab provide us with focused direction.

IATAC has maintained an eagle-eye view over government, industry, and academia's activities aimed at improving cybersecurity. We are committed to the advancement of cybersecurity and IA. The *IAnewsletter* has allowed us the opportunity to highlight innovations and challenges, both of which are important in identifying ways for CS/IA to progress. The Defense Technical Information Center (DTIC) is committed to this also, and CSIAC will be, too. I ask for your active support for DTIC's CSIAC program.

We are passionate about ensuring all are protected against cyber threats, and we thank the countless *IAnewsletter* authors and contributors to IATAC who have shared their perspectives and stories with us. In the transition period, we will still engage with the IA community through our Web site, LinkedIn, Twitter, Wikipedia, and countless other means.

In closing, thank you, everyone, for your support. See you on the high ground!

IATAC: Helping to Tackle Cyber Challenges

by Karen Mercedes Goertzel, Gene Tyler, and Ron Ritchey

We all clearly recognize the good that information communications technology (ICT) has brought to the world—greater access to critical information, faster transactions, and the ability to break down cultural barriers are just a few—but it is hard not to see that humans, in allowing ourselves to become so dependent on ICT, have relinquished a significant amount of control over our own destinies. Take cybersecurity (CS) and information assurance (IA) for example; they have always been difficult to implement for various reasons, some technical, others policy-related. Over the past decade or so, they have presented challenges that have enabled a growing industry to continuously evolve.

Ubiquity and Dependency vs. Security

Because of ICT ubiquity and miniaturization, and with the human dependency on ICT, more—much more—needs to be protected now than ever before. And yet, the characteristics of modern information systems that make them so powerful and versatile are what make them harder than ever to protect. There are just too many ways to subvert them, and too many places where backdoors and vulnerabilities can be found and exploited to bypass those protections that do exist; the Internet has no *Delete* button.

In the past, the worst threats to ICT, in terms of potential intensity and damage, came from disgruntled, revenge-seeking insiders and well-resourced information warriors. Indeed, the Department of Defense's (DoD's) motivation for standing up the Information Assurance Technology Analysis Center (IATAC) was to create a clearinghouse for information on, and a mechanism for research into, nation state-level information warfare.

Now insiders remain a significant threat, but are far more likely to be motivated by greed than resentment (or by a combination of the two). Additionally, external threats are likely to be motivated by greed; well-resourced cybercriminals as well as well-resourced nation states pose as our cyber threats. While cyberterrorists were a theoretical concept in 1996, today they are very real and bent on exploiting our total reliance on the virtual—computers and networks—to operate and control the physical—systems that produce and distribute electrical power, that manage finances, enable transportation, *etc.* Technically-sophisticated terrorists can remain at a safe distance from their targets, yet wreak as much damage and destruction on critical infrastructure as would bombs or other physical attacks—catastrophe by cyberproxy. Consider how Supervisory Control and Data Acquisition systems were once a needed capability, and now we are concerned about the vulnerabilities they bring about. This describes the threat top down.

The threat bottom up, however, is posed by the increasingly technology savvy individuals whose etiquette, ethics, and socialization are produced by excessive "virtual reality." This new "virtual value system" renders these people unable or unwilling to see the damage they cause by their misuse of ICT in pursuit of self-gratification. Today's "human in the loop" is more adept than ever at bypassing ICT security protections, and feels little or no compunction in doing so whenever those protections are inconvenient. Additionally, the anonymity inherent in how many software applications work means users can often bypass security protections without detection.

This is the world in which IATAC has operated since its inception. It is a world in which significant advances have been made in CS and IA, yet in which the most persistent hard problems remain unsolved and new ones come to light as technology evolves. Additionally, the advances that have been made are struggling to keep pace with the threats that emerge alongside them. This article explains IATAC's contributions to meet these challenges head on.

IATAC: A Brief History

Defensive Information Warfare (DIW) was on the minds of many at the Pentagon in the 1990s. In 1994, the then

In 1996, DTIC established its new "virtual IAC"—IATAC—to "provide the DoD a central point of access for information on Information Assurance emerging technologies in system vulnerabilities, research and development, models, and provide the analysis for the development and implementation of effective defense against Information Warfare attacks."

Director of Defense Research and Engineering (DDR&E) asked the Defense Technical Information Center (DTIC) to consider standing up an Information Analysis Center (IAC) to provide DIW analysis. As the Federal Bureau of Investigation (FBI) was zeroing in on fugitive hacker Kevin Mitnick, the Under Secretary of Defense for Acquisition and Technology established a Defense Science Board (DSB) Task Force on Information Warfare-Defense. The DoD issued Directive 3600.1, "Information Operations" while the DSB Task Force completed its report concluding that threats to DoD's networked information systems had dramatically increased the risk that DoD would not be able to carry out its missions. The DSB recommended more than 50 "extraordinary actions" for DoD to defend its systems, networks, and facilities against information warfare attacks.

In 1996, DTIC established its new "virtual IAC"—IATAC—to "provide the DoD a central point of access for information on Information Assurance emerging technologies in system vulnerabilities, research and development, models, and provide the analysis for the development and implementation of effective defense against Information Warfare attacks." During its first year and a half of virtual existence, the IATAC published several reports on modeling and simulation, malicious code, intrusion detection systems, and vulnerability analysis tools, along with the first two issues of what would become its quarterly publication, the *IAnewsletter*.

By 1997, the virtual IATAC had proved its worth, and in May 1998, it was transformed into a bricks-and-mortar operation jointly sponsored by the DDR&E, the then Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C3I])/DoD Chief Information Officer (CIO), Joint Staff Command, Control, Communications and Computers Systems Directorate (J-6), the National Security Agency (NSA), and the Defense Information Systems Agency (DISA). In 1998, DTIC awarded a contract to Booz Allen Hamilton to run the new physical IATAC operation, which it has done since that time. IATAC is currently located in Herndon, VA.

1999 was a busy year for the new IATAC, with increased collection of information on the "insider threat to information systems" and the tools, technologies, and research and development (R&D) focused on detecting and responding to malicious insider activity. In the fall of 1999, the IATAC Technical Area Task (TAT) Program was initiated, enabling IATAC to provide analysis for a broad spectrum of IA R&D technical activities from which all information products generated would be contributed to IATAC's IA knowledge base for access and reuse by organizations across the IA

community. One of IATAC's first TATs called on its subject matter experts (SMEs) to assist the new Joint Task Force-Computer Network Defense (CND) in IA analysis for working groups, integrated product teams, conferences, planning meetings, task forces, *etc.* Over the past 12 years of the TAT program, IATAC has provided similar analysis to organizations across DoD, not just in the areas of IA and CND, but also DIW, communications security, software assurance, and ICT supply chain risk management security.

As DoD's primary IA information broker and information sharing facilitator, IATAC was also called on to provide functional IA analysis for and organize and give presentations at workshops, meetings, conferences, and other events, and to participate in the planning, scenario development, and execution of IA and CND exercises and technology and interoperability demonstrations. IATAC staff provided analysis for key government officials and responded to queries and requests for information, including providing analysis and recommendations for responses to official requests from Congressional committees and subcommittees. In its early years, IATAC began a tradition of developing and delivering training courses on a wide range of IA/CND subjects, at commands and headquarters worldwide.

IATAC TATs would also be put in place to help improve DoD IA/CND processes, to perform and analyze results of risk and vulnerability assessments of systems and software, and to provide analysis for security, test, and evaluation and other certification and accreditation activities. IATAC provided analysis and recommendations for policy development including more than 100 NIST Special Publications (SPs) and more than a dozen NIST Interagency Reports (plus at least one Federal Information Processing Standard). IATAC experts reviewed IA/CND Concepts of Operation (CONOPS), plans, and policies (*e.g.,* DIACAP, Chairman of the Joint Chiefs of Staff Instruction 6510.01E "IA and CND", prototyped IA/CND capabilities and tools, and developed IA-related prototype Web presences for numerous military and defense organizations.

IATAC provided analysis for policy development including more than 100 NIST Special Publications and more than a dozen NIST Interagency Reports.

IATAC has collaborated with NIST, DISA, and NSA in developing NIST SP 800-126 defining Security Content Automation Protocol (SCAP) Version 1.0, marking the beginning of IATAC's ongoing involvement in the Information Assurance Automation Program at NIST. In addition to helping enhance and expand the original SCAP specifications, IATAC assisted in the development and validation of SCAP content, analyzed raw Common Vulnerabilities and Exposures and Common Configuration Enumeration descriptions, and assigned Common Vulnerability Scoring System Version 2 scores and Common Weakness Enumeration or Common Platform Enumerations (CPE) vulnerability type designations. IATAC also helped develop the official CPE product dictionary; helped establish the SCAP validation lab accreditation program under the National Voluntary Laboratory Accreditation Program; and enhanced the National Vulnerability Database (NVD), including the transition of NVD entries to standard SCAP-compliant CPE format. IATAC has also provided analysis for the National Checklist Program database, the Federal Desktop Core Configuration (FDCC) SCAP content, and provided IA and cyber analysis for the FDCC SCAP validation of Microsoft components over the years.

These successes have often been attributed to IATAC's leadership. Since its inception, IATAC has had instrumental directors who have developed satellite offices to grow IATAC services to Combatant Commands and increase IATAC's TAT portfolio. All of the former directors remain closely affiliated with the program today and continue to help strengthen IATAC's program. Our directors' previous work experiences have strengthed IATAC's relationships with several key organizations.

For example, IATAC was instrumental in planning and providing analysis for site visits of facilities such as the Joint Task Force-Computer Network Operations (JTF-CNO) operation at the Pentagon, the DoD CERT, and the DISA Global Network Operations and Security Center, as well as providing analysis and background information for briefings and discussions for senior officials and delegations from NATO and U.S. allies' and coalition partners' defense establishments in North America, Europe, and Australia. While providing analysis for the JTF-CNO/J5 Foreign Disclosure and International Affairs Office, IATAC provided analysis essential to finalizing a key piece of Defense Intelligence Agency (DIA) policy that resolved longstanding obstacles to U.S. information sharing with its allies.

In 2002, the Director of Information Assurance in the Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD-NII) announced a new initiative for sharing ITC and IA product evaluations across DoD. IATAC provided the analysis and background information for a program that evolved into the DoD Commercial Innovation and Integration program, and ultimately into DoD IA Connect. This program continues to facilitate technology demonstrations between industry and DoD, which is a key step in advancing our national IA strategy.

In 2002, IATAC also assisted the JTF-CNO Law Enforcement and Counter-Intelligence Center (LECIC) and FBI cybercrime investigators in their analysis of the first distributed denial of service (DDOS) attack on the Internet's 13 domain root servers. IATAC also provided analysis for the LECIC in meetings with NSA and worked with the FBI, LECIC, and the Naval Criminal Investigative Service in their ongoing investigation of Titan Rain and other cyber intrusions of DoD systems, including Internet Relay Chat botnet intrusions. IATAC helped advance a joint LECIC/JTF-CNO-J2 threat matrix for quantifying and profiling hacker groups that threaten DoD networks. IATAC also provided analysis for JTF-CNO efforts to understand and anticipate cyber and malware attacks, performed trend analyses, attribution analyses, and documentation of botnet activity in the Global Information Grid, and studied network intrusions and emerging computer worms and viruses to identify potential threats to DoD networks, as well as emerging hacker tools.

As its TAT program grew over the next few years, IATAC provided analysis for virtually every DoD Combatant Command, Service, and Agency, as well as numerous civilian agencies, and has provided expertise for policies, risk management plans, CONOPS, design documents, implementation plans, and/or accreditation plans for many major defense and civilian government information systems and entities. These organizations include the Global Combat Support System, USTRANSCOM Global C4S Coordination Center, Defense Advanced Research Projects Agency's Total Information Awareness, the Federal Performance Key Indicator Cross Certification Bridge, DISA's Wireless Security Support Program, the DIA/CIA/NSA Joint Information Operations Program, the Air Force Research Laboratory, USPACOM's IA/NetOps Analysis Cell, the Air Force Information Operations Center, the DoD enterprise-wide IA and CND solutions steering group, and many others.

Under one of its TATs, IATAC provided analysis for the development of the Classified and Unclassified versions of DTIC's Total Electronic Migration System (TEMS) and deployed prototype TEMS systems at IATAC headquarters, and at satellite sites in Atlanta, GA and Aberdeen, MD. In the fall of 2006, the one millionth record was added to TEMS.

In the wake of a series of major cyberattacks in 2007, IATAC cyber threat experts helped provide analysis for a diagram depicting cyber threat "social networks" for the Commander and Deputy Commander of USSTRATCOM/Joint Functional Component Command-Network Warfare and representatives of the National Security Council, Department of Justice, and other cyber threat mission partners. This Cyber Threat Social Network Diagram enabled planning and execution of military CNO. In the same year, IATAC was tasked by DIA, after regional and country experts in DoD and other government agencies were targeted by a series of spoofed e-mails to analyze the attack targets and discover the attacker's tactics, techniques, and procedures. After the second major DDOS attack on the 13 Internet domain root servers in 2007, IATAC provided the DoD CIO's Internet Governance team with recommendations for securing the Internet's Domain Name Service.

That same year, IATAC provided analysis to help secure the ITC infrastructure used by the U.S. Army Corps of Engineers for recording the results of their post-Hurricane Katrina nation-wide levee inspections and integrity assessments. IATAC has played a role in natural disasters. A few years later, in March 2011, IATAC provided analysis for USPACOM's Operation Tomodachi disaster relief effort in Fukushima Prefecture, Japan following the 8.9 magnitude earthquake and subsequent tsunami, by helping establish the All Partners Access Network virtual workspace and data depository to enhance secure collaboration and relief effort coordination between Japanese and U.S. civil government and military authorities.

In 2008, IATAC experts participated in the development of a Cyber Security and IA Science and Technology Roadmap requested from the then DDR&E by the Deputy Secretary of Defense and his Advisory Working Group. In 2010, IATAC stood up its own Living Lab adaptive user environment, for development, observation, and experimentation with IA technologies emerging from research labs before they transition into operational use. The Living Lab provides IA and cyber analysis for the National Information Assurance Research Laboratory, (*e.g.,* in a pilot of host integrity and multi-factor authentication R&D [tokens, biometrics, and passwords]).

In 2011, IATAC also provided analysis for USSTRATCOM in developing a prototype to demonstrate the presence and exploitability of vulnerabilities in classified systems of interest. IATAC incident response and remediation analysts also performed intrusion analysis helping to identify potential vulnerabilities, threats, and subsequently bolster network security.

Creating CS/IA Resources for All

Throughout the existence of the IATAC program, its SMEs have produced (and updated) numerous information products, including critical reviews and technology assessments (CRs/TAs), (*e.g.,* on Net-Centric Warfare, Biotechnology, IA Metrics, Data Mining, Computer Forensics, and Biometrics), IA Tools Reports (*e.g.,* on Firewalls, Intrusion Detection and Prevention Systems, Antimalware tools, and Vulnerability Assessment tools), and State-of-the-Art Reports (SOARs) (*e.g.,* on malicious code, IA modeling and simulation, IA/Information Operations visualization, and IA/CND needs and plans across DoD).

To facilitate the collection, analysis, and dissemination of CS/IA information, IATAC evolved a number of free products to provide the entire IA community with up-to-date, relevant information, and to foster collaboration. To date, IATAC publishes the IA Digest, a weekly news summary providing links to relevant CS/IA articles; the Cyber Events Calendar, an all-inclusive summary of CS/IA conferences and symposia; the Research Update, a quarterly mailing for academic and R&D communities that provides a snapshot of recent IA scientific and technical information collected, and the *IAnewsletter*, IATAC's quarterly magazine that features CS/IA articles and has over 50,000 total distribution quarterly. Additionally, IATAC maintains a presence on LinkedIn and DoDTechipedia, DoD's collaboration portal, to better connect with IA experts and professionals, and to strengthen its Technical Inquiries program, which enables customers to take advantage of 4 hours of free CS/IA research.

In July 2007, IATAC culminated a year-long joint study with the Data and Analysis Center for Software on the increasingly critical problem of information systems made vulnerable by their untrustworthy, unreliable software. The outcome of the research was DTIC's first-ever publicly-releasable SOAR, Software Security Assurance. The SOAR, which would ultimately be downloaded or ordered in hardcopy by more than 700,000 readers, would be cited in dozens of books, theses, whitepapers, and reports, would become recommended or required reading in numerous university courses, and would be referenced for the body of knowledge used in developing the qualifying examination for the International Information Systems Security Certification Consortium, Inc., Certified Secure Software Lifecycle Professional certification. This resource provides an in-depth analysis of how processes, techniques, and tools throughout the software life cycle can result in vulnerable software, and depicts the landscape of government, industry, and academic initiatives and research to advance practices, techniques, and tools in an effort to improve the security of the software that results.

A year later, in 2008, IATAC published its long-awaited SOAR on The Insider Threat to Information Systems, one of the most intractable "hard problems" of IA and CS. The following year, to assist the DIAP as well as others in government, industry, and academia, IATAC published an IA Policy Chart that organized and emphasized relationships among the proliferation of DoD, Intelligence Community (IC), and civilian government IA policies. In 2009, IATAC also published its second publicly-releasable SOAR on the challenging problem of Measuring Cyber Security and Information Assurance. In August 2010, IATAC published its final SOAR on Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain. By April 2011, the SOAR had been requested for use as a textbook in classes at the National Defense University and the Army Logistics University.

Throughout its operation, IATAC has established relationships with other IACs, and with numerous IA and CS experts and research organizations not only in government, but also in academia and the private sector, including The Institute for Applied Network Security, a center that promotes IA education, particularly at community colleges, called CyberWatch; Carnegie Mellon University's CyLab; and Purdue University's Center for Education and Research in Information Assurance and Security, to name a few. These relationships have been vital to IATAC in providing the most accurate and relevant CS/IA resources.

Since its inception in 1996, IATAC has never lost sight of its primary mission: the collection, analysis, and dissemination of IA-related scientific and technical information for DoD's defensive information warfare, IA, and CS efforts. We will conclude our history of IATAC with a few statistics that attest to the success it has achieved in providing critical information to the CS/IA community—

- Total number of items in the IATAC IA Library
  - May 1998: 0
  - November 2011: 22,915
- Total number of IATAC SOARs disseminated since 1998: 906,000
- Total number of IATAC IA Tools reports disseminated since 1998: 81,500
- Total number of subscribers on the *IAnewsletter* mailing list:
  - May 1998: 0
  - November 2011: more than 9,100
  - Total annual distribution: 214,000
  - Total distribution: over 1.3M

The Future of CS/IA as IATAC Sunsets

In May 2010, DTIC awarded the Software, Networks, Information, and Modeling & Simulation (SNIM) contract to nine primes. This contract vehicle combines the TAT activities of three IACs including IATAC. Just over a year later, in June 2011, DTIC released its request for proposal for the Cyber Security and Information Systems Information Analysis Center (CSIAC), which will be a small-business set-aside. As SNIM did, CSIAC will consolidate the product and service offerings of IATAC with two other IACs. This transition will likely take place in early 2012. IATAC expects to be engaged in assisting the transition of its product and service offerings to the CSIAC, and it will continue providing CS/IA analysis across the government under its existing TATs until May 2013.

There are some ongoing intractable IA and CS "hard problems" that the new CSIAC will likely be called on to help DoD and the federal government understand and address—

- Security for small, highly mobile computing devices;

- Security of "the Cloud" in which data and applications accessed by those devices will be located;
- Advanced persistent threat;
- Security of computers and networks used to control physical systems and processes;
- Security of the ICT supply chain: Stuxnet proved the reality of APTs that leverage the supply chain for the components of targeted systems; and
- Self-protecting data: Information security needs to evolve from reliance on traditional "data at rest" and "data in transit" protections (*e.g.*, externally-enforced access controls, network/session-level encryption) to embedded access controls that overcome the impracticalities of digital rights management systems while preserving their intention.

Two far larger challenges underpin these (and most other) IA and CS "hard problems"—

- **Judging and communicating trustworthiness**—How does one judge and communicate trustworthiness, not just of humans, but of all logic-bearing or information-bearing entities in a computer/network system? What truly meaningful "evidence" can one entity provide to another to enable that second entity to judge that the first is trustworthy enough for the job it is expected to perform at the time and in the context in which it is expected to perform it? And how can that trustworthiness be effectively reassessed, and entity-to-entity relationships and expectations adjusted, as circumstances change?
- **Anticipating and surviving the threat**—Much work has been done in the area of "survivability," but much more is needed. It has to start with a psychological shift from security based on the "understand-protect-monitor-react" approach to individual threats, to security based on the ability to survive all threats. And, what definition(s) should be used for survivability? APTs are already pushing the envelope with regard to leveraging artificial intelligence for reconnaissance, deception, adaptability, and survivability. Defenders need to not only catch up but outpace these advances.

In reality, these hardest-of-hard problems have existed for as long as ICT systems have been in existence. Given the limits on resources for IA and CS, it is likely these problems will persist long into the future.

A major step forward would be to reset our priorities. Organizations and individuals need to recognize just how dependent they have become on ICT. It may be a truth universally acknowledged that ICT can be intentionally subverted or sabotaged, but those who depend on ICT must act with the understanding that once that subversion or sabotage occurs, ICT cannot be trusted to operate as it should when it should. This will prevent us from becoming virtual slaves to the technology that serves us, especially since the next big APT could easily derail a critical mission, drive a business into bankruptcy, or destroy a life. In these days of shrinking budgets, we need to compensate by becoming twice as persistent and 10 times as creative as our adversaries. CSIAC will be an important institution for sharing information about how we can more creatively and imaginatively address these threats with far fewer resources. We encourage you to become engaged with CSIAC. ■

About the Authors

Karen Mercedes Goertzel | is a Certified Information Systems Security Professional and leads Booz Allen's Information Security Research and Technology Intelligence Service. An expert in software assurance, ICT supply chain risk management, assured information sharing, and the insider threat to information systems, she has performed in-depth research and analysis for customers in the DoD, the Intelligence Community, civil agencies, and industry in the U.S., U.K., NATO, Australia, and Canada. She was lead author/editor of Information Assurance Technology Analysis Center's State-of-the-Art Report on ICT Supply Chain Risk Management, the Insider Threat to Information Systems, and Software Assurance as well as a number of other IATAC information products and peer-reviewed journal articles and conference papers on these and other CS/IA topics. She can be contacted at *iatac@dtic.com*.

Gene Tyler | is a Booz Allen employee and is the IATAC director. He is a retired U.S. Army combat veteran who served over 35 years. He has extensive combat and operational deployment experience with two tours of duty supporting U.S. initiatives in the Republic of Vietnam and the Bosnian peace efforts, and an operational and command deployment as a Combined JTF commander in the Middle East. Mr. Tyler has extensive staff and command experience both overseas and on the Office of Secretary of Defense (OSD) staff. In his last military assignment, Mr. Tyler served on the OSD staff as the DIAP Director. He holds multiple graduate degrees and is a distinguished graduate of the national level Senior Service College – the Industrial College of the Armed Forces. He has also been selected as an Officer Candidate School Hall of Fame Member. He can be contacted at *iatac@dtic.com*.

Ron Ritchey, Ph.D. | is Chief Scientist of the IATAC and a leading technologist specializing in IA with over 20 years experience working within the ICT industry. He is widely published on network security topics including co-authoring recent books on software assurance and insider threat. He has authored courses on computer security that have been taught across the country and is a faculty member of the System Administration, Networking, and Security Institute, the Institute for Applied Network Security, and George Mason University (GMU). Dr. Ritchey holds M.B.A and B.A. degrees in computer science from GMU and a Ph.D. in IT from their School of Information Technology and Engineering. He can be contacted at *iatac@dtic.com*.

Army Cyber Command: Redefining IA Compliance as Part of Operationalizing Cyber

by LTG Rhett A. Hernandez and LTC Christopher R. Quick

Cyberspace has and will continue to change the way we all conduct our Profession of Arms—from the infantryman to the signaler and from the intelligence analyst to the commander in the field. Global connectivity and the speed at which information is transmitted around the Earth have fundamentally altered our world, and we cannot go back to how things were. Technology continues to rapidly evolve to meet today's threats while simultaneously building to the future; we must understand the drivers for this change and stay ahead of their implications. Nothing is more paramount in this venture than understanding and mitigating risk. We can accomplish this by implementing standards, correcting deficiencies, and enforcing modes of user behavior, currently known as compliance. The bedrock of our Army is standards and discipline, and we must be disciplined in the cyberspace domain.

Compliance in information assurance (IA) is one of the Army Cyber Command's most pressing and important mission imperatives. It is a multi-dimensional term subject to wide interpretation in its application. Driving this vital imperative are cyberspace threats that are real, growing, sophisticated, and evolving. As we work to take full advantage of cyberspace's potential, we must recognize existing and future threats and appreciate their ability to prevent us from operating freely. Threats include a wide set of actors with digital devices or computers trying to improperly access our enterprise with nefarious intent. Trend analysis indicates the number and sophistication of attempts to exploit our networks will continue to increase and mature. We must anticipate the evolution of these threats. Every time we enter the network, regardless of where we are, we are in a contested environment in which we must fight to maintain our freedom to operate.

Since its creation, the Army Cyber Command has actively focused on operationalizing computer network operations. IA compliance is a key part of this process; however, there are unique challenges in doing so, including: the volume of IA threats and vulnerabilities; the escalating pace and sophistication of emerging threats; the distributed and dispersed state of current Army networks; a general lack of security training and awareness; and a traditional lack of leadership, understanding, and involvement in actively implementing required IA operations. In addition, the Command has worked to reduce the frequency and systemic causes of costly IA compliance failures, such as unauthorized disclosures of classified information (UDCI)—formerly known as "spillage." In all, operational emphasis on IA compliance has led to tangible improvements in security and user awareness. Much, however, is still required of the Army Cyber Command, the cyberspace community of interest, and Army leadership to mitigate risk and deny adversaries access to the Army's sensitive information.

Why IA Compliance?

The better question to ask is, "Why compliance with Army orders and directives?" The primary reason for enforcing Army-wide standards and user norms is the need for a strong defense. Protecting information and guaranteeing transportation through cyberspace is essential to how our Army fights. The ability to operate when degraded or disrupted provides significant advantages to the side that can gain, protect, and exploit advantages in the contested cyberspace domain. The advantage will go to whoever best mitigates the loss of intellectual capital and reduces the number of vulnerabilities.

In some cases, improved defense results directly from short-term actions taken to diminish known threats, such as the application of a vendor patch. In other cases, improved defense results from the gradual implementation of enterprise-wide applications that move the LandWarNet (the Army's network) toward a more uniform and interoperable network. For example, migrating to a common Windows

platform or synchronizing the tuning of a host-based security system may not give the immediate appearance of defense, but these important actions promote a more automated and responsive network. Without these common configurations, the network cannot effectively feed the emerging common operational pictures, such as information technology asset management or continuous monitoring. We can neither afford the loss of critical information nor the cost of remediation. A clear example of this is in the area of UDCI, where an entirely avoidable act can result in a sizeable remediation price tag for the unit involved. This year, remediation costs exceeded $700,000, which is unacceptable.

Most important, however, is that complying with orders and directives is not voluntary. As with any Army operation or task, orders and directives must be followed. Just as with any mission or operation, failure to accomplish assigned tasks can jeopardize the overall mission. This is critically important in cyberspace operations because cyber enables mission command.

What is Army Cyber Command Doing?

The Army Cyber Command is actively moving forward with operationalizing IA compliance by regimenting the orders process and helping commanders mitigate risk by prioritizing vulnerability remediation to address the most critical enterprise vulnerabilities first. This process allows field commanders to see risks in operational terms so that they can understand impacts to their units and take action based on operational needs.

The Army Cyber Command is actively moving forward with operationalizing IA compliance by regimenting the orders process and helping commanders mitigate risk by prioritizing vulnerability remediation to address the most critical enterprise vulnerabilities first.

Consider the case of the UDCIs described above. Since reaching a monthly high in February 2011, poor user behavior has declined 50% by the end of October 2011. Command emphasis and outreach reduced the frequency and severity of these events; however, more work is required. Commanders at all levels have come together with a common sense of urgency to correct the problem.

Where orders implementation is concerned, one process in particular is putting a fine point on compliance. Dubbed the High Risk Vulnerability List, this new breed of order identifies the most widespread and potentially debilitating vulnerabilities in the Army and mandates they be addressed immediately. Their status is reviewed weekly, with focus on a manageable set of vulnerabilities versus the full continuum of active vendor patches. Anecdotal responses from the field have been positive as this High Risk order establishes a common priority of effort based on command direction.

Cyberspace operations orders also work well in high profile cases where the Army must act immediately and decisively in the face of emerging threats. On the heels of the Wikileaks incident in late 2010, for example, the Army Cyber Command issued the single codifying order that aligned all mitigation actions. Units subsequently reported full compliance within weeks of the release of the order. This single recognized orders process continues to pay dividends across a broad range of deliberate actions, from enterprise

The Army Cyber Command has also established a recurring command forum for the assessment of other compliance indicators.

e-mail to the patching and scanning of Army systems.

The Army Cyber Command has also established a recurring command forum for the assessment of other compliance indicators. The monthly Cyberspace Operations Readiness Report brings all components together to discuss the status of orders implementation, cybersecurity training, high risk vulnerability implementation, and the results of external inspection. It is this last compliance element where the Army Cyber Command stands poised to make a fundamental difference. For too long, the Army's information security inspections have been "fire-and-forget" events that might have received attention early on, but then faded into obscurity soon afterward. The Army Cyber Command has taken the lead role in de-conflicting the numerous IA inspections pending at any given time by various organizations (*e.g.*, Defense Information Systems Agency, Command Cyber Readiness Inspections, Inspector General, and Army G3), and is aligning the full Army audience to a concise list of candidate sites. The Army Cyber Command will also ensure the thorough follow-up of any significant findings through sustained contact with the affected organizations.

In addition to influencing assessments and their results, the Army Cyber Command wants to improve the integrity of its IA compliance reports and statistics, both through manual and automated means. Today, compliance reporting is largely done through semi-automated methods (*e.g.*, machine scanning with "stubby pencil" analysis), but command emphasis is now on a fully automated reporting structure. With the enterprise tools now available to perform these scanning and reporting functions, it makes little sense to wait for the "ultimate" reporting structure. Rather, the Army Cyber Command is reaching aggressively for the low hanging fruit—things that can be leveraged today.

The Way Ahead

As with all operations, standards must be clear and enforced. Discipline is a military hallmark, and we must be as disciplined on our network as we are with our weapon systems. By making IA compliance a commander's priority exercised through educated users who understand their role in the defense of the network, we will better promote a strong defense of our networks. The continued cultivation of an environment where the standard is strong compliance, protection of information, and guaranteed transport of information through cyberspace, will make serious and lasting improvements for the security and efficiency of Army networks.

While resourcing and technical constraints deter rapid, uniform compliance, the Army Cyber Command will continue to push to change the conditions and mindset within the Army so compliance becomes second nature. As in any defense, adversaries will find and exploit our weakness. To counter this, we must treat compliance like a weapon system and be ready to defend and protect against a threat that is real, growing, and evolving. In the end, compliance with orders and directives in IA is no different than with any Army operation, task, or directive. Leaders need to actively engage to ensure mission accomplishment, no matter the operational domain. Maintaining the freedom to operate in cyberspace is everyone's business. The Army Cyber Command is committed to supporting commands and enabling mission command. ■

About the Authors

LTG Rhett A. Hernandez | is currently the Commanding General, U.S. Army Cyber Command / Second Army at Fort Belvoir, VA. His commands have ranged from the battery level with 2nd Battalion, 33rd Field Artillery and 1st Battalion, 5th Field Artillery to Battalion level with 1st Battalion, 14th Field Artillery, later re-designated 3rd Battalion, 16th Field Artillery to Brigade level command as the Commander of Division Artillery, 4th Infantry Division (Mechanized), Fort Hood, TX. LTG Hernandez also served as the Assistant Division Commander (Support), 1st Armored Division, United States Army Europe and Seventh Army, Germany and OPERATION IRAQI FREEDOM, and the Commanding General, U.S. Army Human Resources Command, Alexandria, VA. LTG Hernandez holds a B.S. degree from the U.S. Military Academy, an M.Ed. degree in Systems Engineering from the University of Virginia, and an M.S. degree in National Security and Strategic Studies from the National War College, Fort Leslie J. McNair, Washington, DC. He can be contacted at *iatac@dtic.com*.

LTC Christopher R. Quick | is currently the Director of Strategic Communications for the U.S. Army Cyber Command / Second Army at Fort Belvoir, VA. His assignments include Fire Support Officer, Battery Executive Officer, Brigade Assistant Operations Officer, and Brigade Fire Direction Officer. He commanded a Battery with 1st Battalion, 17th Field Artillery. He served in the 41st Signal Battalion, 1st Signal Brigade as a Battalion Automations Officer. LTC Quick served as Brigade Information Operations Officer with the 2nd Brigade, 101st Airborne, where he served a tour in Iraq. He has served on the Army Staff within the Army G3/5/7 in DAMO-ODI and served on the Army Cyber Task Forces as the lead action officer for the development of Army Cyber Command. LTC Quick holds a B.S. degree from Park University in Kansas City, MO and an M.S in Computer Science and another in Information Operations from the Naval Post Graduate School in Monterey, CA. He can be contacted at *iatac@dtic.com*.

Ask the Expert

by Ed Moyle

Five Disruptive Technologies Security IA Pros Should Address

Sometimes we in information assurance (IA) do not pay careful attention to disruptive technological adoption patterns as other disciplines. Perhaps we do this because disruption does not change our focus the same way it does for other technology disciplines.

As new technologies emerge and push existing technologies out of relevancy, other disciplines generally shift their focus to the new technology. Because the disruptive technology becomes rapidly cheaper/better to deploy as it is refined, being a good technologist means figuring out how to adopt and incorporate the new technology in an advantageous way.

In IA, however, the pattern is a little different. We have to keep new and old technologies in our sights, as long as they both support the mission. For example, ask yourself from an assurance standpoint, at what point do I stop securing what is fielded? You do not stop, right? If a given technology is critical to the mission, it is in scope to secure, whether it is a new disruptive technology or an old legacy technology being disrupted.

We have to keep new and old technologies in our sights, as long as they both support the mission.

Scope and Impact are Different

To create a rough parallel, imagine you lived and worked when horse drawn carriages were being replaced by automobiles. The trajectory of auto adoption followed the pattern of a disruptive innovation curve in an almost textbook-like fashion. If you lived in that time period and were in the business of providing transportation, chances are you were focused on automobiles, not the horse and buggy; however, what if your job was to write traffic laws to keep the roads safe? Because the vehicles shared the same road, you needed to address both, at least until the buggy was in such rare use that it was effectively negligible to the safety equation.

Since the scope of what we need to address from an assurance standpoint tends to not change in response to disruptive technology, the temptation from IA is to overlook the phenomenon entirely. This can be problematic, though, because security tools themselves are subject to the same patterns of adoption as other technologies, meaning disruptive technologies offer opportunities for practitioners to take advantage in new, better, and/or cheaper ways.

So from a practitioner standpoint, it is important for us to be aware of—and plan around—disruptive innovations, even when impacts are not felt as directly in our discipline as in others.

Technologies to Have on Your Radar

With that in mind, below are a few disruptive technologies that IA professionals should have on their radar, either because they affect current security practices or because they directly impact core tools in IA—

- **Virtualization**—Virtualization technologies displace dedicated physical hardware. Savvy IA professionals should take note because of the impact virtualization has on widely-deployed security tools. Specifically, as communication shifts from network-based communication to backplane-based communication, the visibility and capability of existing security tools (*e.g.,* network-based intrusion detection and firewalls) is altered.
- **Cloud**—Many organizations are moving away from on-premise infrastructure to off-premise, service-based models. As a result of

▷▷ *continued on page 16*

Training IA Experts of Tomorrow

by Victoria Victor

The National Science Center (NSC), created under congressional authority, Public Law 99-145 in 1985, is a public-private partnership between the Army (NSC-Army) and a non-profit organization. The NSC-Army recently launched the first phase of a comprehensive cybersecurity educational program for K-12 students and teachers, called Cyber Ops. The Cyber Ops program mission, like NSC's Mobile Discovery Centers, is to excite America's youth about science, technology, engineering, and math (STEM) through engaging educational outreach activities.

Cyber Ops seeks to address two critical needs that arose with the rapid expansion of cyberspace: the need for a well-trained workforce that can meet tomorrow's cybersecurity demands and the need to ensure the online safety and security of America's youth.

Need for a Cybersecurity Workforce to Meet Tomorrow's Cybersecurity Demands

The intent of the Cyber Ops program is to leverage gaming, modeling, and simulated environments to provide cybersecurity and information assurance (IA) content that makes learning about technology fun, while providing students with a STEM solid foundation to ensure that the future workforce is more cyber savvy and the need for skilled cybersecurity experts is met.

Cyberspace is a global domain of interconnected networks using information-communication technologies to create and exchange digital data and media world-wide. Low-cost Internet access technology and easy-to-use digital authoring tools make communication, collaboration, and access to information and social media content easier than ever before.

Unfortunately, as access to cyberspace has increased, so have threats and attacks against cyber technologies. With millions of attacks against the nation's networks and infrastructure occurring on a daily basis, economic impact from cyber attacks can range from $13 to $200 billion annually. [1] By 2020, it is estimated that there will be almost 3 billion Internet users, driving massive new investments in infrastructure, technology, and new security architectures, as well as an increased demand for cybersecurity experts to detect, defend against, and mitigate these attacks. [2]

According to James Gosler, a government cybersecurity specialist, the United States has a severe shortage of computer security specialists, estimating that while there are only about 1,000 people in the entire United States with the sophisticated skills needed for the most demanding cyberdefense tasks, 20,000 to 30,000 skilled experts are needed. [3] Educators and security experts alike have identified the growing gap between use of cyber technologies and knowledge of cybersecurity best practices as a major weakness in the workforce that increases the nation's vulnerability to cyber attack.

Dena Haritos Tsamitis, director of Carnegie Mellon University's Information Networking Institute and education, training, and outreach at the university's CyLab, states that ensuring today's students receive STEM education that includes cybersecurity and IA is essential for developing a skilled workforce capable of fighting against cyber warfare launched against large organizations, national infrastructure, and federal agencies. [4]

Need to Ensure Online Safety and Security of America's Youth

While the need to create a cyber-savvy workforce for our nation's future is a serious ongoing concern, a greater immediate concern is the risk the nation's children face from cyber attacks. To meet this need, the Cyber Ops educational program focuses on three content areas, which leaders in cyber education agree comprise a comprehensive cyber curricula for children: cybersecurity, cybersafety, and cyberethics (C3).

According to some analyses, more than 80% of teenagers in the United States have access to the Internet at

school, home, and *via* mobile devices and are spending as many as 6 hours a day using Web technology. [5] They routinely interact with "invisible others" *via* smartphones, online games, e-mail, and social media Web sites.

While kids and teens have embraced the digital world with real intensity, most children who access the Internet do not realize the risks involved with failing to protect confidential and personal data online. Without an understanding of the dangers involved in Internet usage, many children unwittingly expose their devices and themselves to viruses, hackers, identity thieves, social engineers, cyber bullies, and cyber stalkers. Children can also be guilty of unethical online behavior, including pirating software, games, and music from online sources because they do not understand the legal ramifications associated with it.

The 2011 edition of State of K–12 Cyberethics, Cybersafety, and Cybersecurity Curriculum in the U.S. Survey, states that America's schools are ill-prepared to teach children the basics of online safety, security, and ethics—skills that are, according to Michael Kaiser, executive director of the National Cyber Security Alliance, as important in today's digital age as math, reading, and writing. [6]

A 2010 survey conducted by Carnegie Mellon University's Information Networking Institute affirms that not only are students not receiving online safety, security, and ethics as an integral part of their STEM education, teachers are not getting adequate training in online safety topics. [7] More than one-third of teachers were found to have received 0 hours of professional development training by their school districts in issues related to online safety, security, and ethics in the past year. [8]

As a result, there is a critical need for new curricula and teacher training that will teach children how to be safe and secure online, make good decisions about their online behavior, and use technology responsibly that the Cyber Ops education program can meet.

The Cyber Ops Education Program

The goal of NSC's Cyber Ops educational program is to provide children of all ages with a solid foundation in technology and IA concepts in support of STEM, as well as the information they need to be safe and secure online. Available *via* the NSC Web site, the Cyber Ops planned curricula will be developed in four separate program components for grades K-3, 4-6, 6-9, and 9-12. Each component will include a series of individual modules for each topic within each C3 content area. For example, cybersecurity content will include modules for cyber technologies, cyber communication, malware, and cyber careers, focused on in-depth information and best practices related to using the Internet and mobile technologies in a safe and secure manner.

Each module will consist of instructional segments designed to meet specified learning objectives and to build on one another. The content will increase in depth and detail moving from awareness, through comprehension and application, to analysis and synthesis. The instructional strategies employed will be increasingly more sophisticated, providing additional challenges and opportunities to demonstrate understanding as the grade level increases. Content will be presented using engaging scenarios and fun reinforcement activities and will employ a wide variety of multimedia elements, including graphics, music, voice-over, animations, and interactions.

Key concepts presented in a module will be reinforced through an accompanying interactive game, which will enable students to apply age-appropriate, problem-solving skills and deductive reasoning to accomplish the game objectives. As additional modules are developed for the program, the games may be incorporated into a larger, more robust format, structured in levels corresponding to grade groups, and organized by content area and topic. Students will have the opportunity to challenge their knowledge at each game level to receive rewards for completion as they progress through the Cyber Ops program content and academic grades. Virtual rewards, or those provided by identified sponsors, will be distributed based on points accumulated.

Cybersecurity—Malware for Grades 6-9

The first academic offerings developed for NSC by the Information Assurance Technology Analysis Center (IATAC), as part of the larger planned Cyber Ops curricula, are a multimedia comic book and an accompanying interactive mystery game for students in grades 6-9 on the critical topic of malware. Available online from the NSC Web site, the Flash-based Malware module and game use a scenario-based approach to provide students with in-depth information about the dangers of malware and best practices they can employ to protect themselves from the threats and vulnerabilities that exist in today's technological world.

The Malware module communicates the content using an engaging, interactive comic book format. As the student navigates through the comic book, age-appropriate characters talk with one another about the dangers of malware. These discussions occur in a variety of environments where malware can exist, including school, home, and an Internet cafe. This dialog provides key information that students need to protect themselves, their friends, and their families from exploitation by malware when using Web technologies. It also helps students differentiate between malware types, identify the risks and vulnerabilities involved with using technology, and understand how devices can be affected by malware. Other topics explored include social engineering, personal information privacy, and social media use. Cybersecurity terminology and malware

identification concepts are reinforced through fun and engaging activities, including crossword puzzles, knowledge check questions, and matching exercises.

The accompanying mystery game presents three "cases" involving a malware attack in a virtual town. Navigating the multimedia-rich environment from an interactive map, the student investigates locations in the town and selects objects to discover clues about the malware infection. One of the locations in the town is a library where students can access a variety of resources, including virtual books, magazines, and computer files, to obtain information about malware that may be needed to solve the mystery. Some of the objects in the locations are "red herrings," while others provide information reinforcing key concepts from the Malware module. Upon discovering a clue, the student must decide whether or not to place it in his or her "clue card." Once all of the correct clues have been discovered, the student must correctly identify the malware type and the best practices for preventing this type of malware infection in the future. All three cases must be solved to win the game.

NSC's National STEM Education Outreach

In addition to the Cyber Ops educational program, NSC's effort in national STEM education, which reaches over 100,000 students annually, includes the Junior Reserve Officers' Training Corps summer camp and in-school programs. These programs provide STEM curriculum and materials for activities that involve learning by doing, such as constructing battery-powered cars.

NSC also takes science on the road with its Mobile Discovery Centers. Housed in 18-wheelers, the mobile centers travel across the country, presenting programs designed to show young people that studying science and math is fun as well as essential to their future.

For more information about the NSC and the Cyber Ops educational program, visit *http://www.nationalsciencecenter.org.* ■

About the Author

Victoria Victor | holds a Ph.D. in Education from Capella University, specializing in Instructional Design for Online Learners. Dr. Victor led the IATAC team that designed NSC's Cyber Ops Education Program plan and developed the Malware module and mystery game. Dr. Victor has been involved in the education of children and adults, as both a teacher and a curriculum developer, for over 25 years.

References

1. (2011). U.S. Federal Cybersecurity Forecast 2010-2015. Market Research Data.
2. *Ibid.*
3. Gjelten, T. (2010). Cyberwarrior Shortage Threatens U.S. Security. NPR News.
4. (2011). K-12 STEM Initiatives and Cybersecurity Education. National Institute of Standards and Technology.
5. (2008). Teens Online. The Henry J. Kaiser Family Foundation.
6. (2011). 2011 State of Cyberethics, Cybersafety, and Cybersecurity Curriculum in the U.S. Survey. Microsoft News Center.
7. Kaiser, M. (2011). America's K-12 Schools Not Preparing Kids for Digital Age. Microsoft News Center.
8. *Ibid.*

▷ *continued from page 13*

ASK THE EXPERT

cloud adoption, architectural changes can impact the security of the environment.

- **Mobile Authentication**—The historical "gold standard" for two-factor, the hardware one-time password, is being displaced by solutions that leverage employee-carried mobile devices as an authentication factor (*e.g.,* Android and iOS based soft tokens plus SMS-based systems). The drivers for this are largely economical since provisioning is often handled by employees without organizational involvement.
- **Remote Bulk Storage**—File sharing tools, like DropBox, are rapidly displacing portable storage devices (*e.g.,* USBs). Many organizations have invested heavily in locking down portable storage, which decreases the risk from incidents like exportation of large amounts of classified data; however, remote network-based services open up a new threat vector.
- **Personal-liable Devices**—More and more, personal-liable devices are being used in lieu of managed endpoints provisioned and secured by technical security teams. If undertaking this strategy, IA professionals must ensure that appropriate security controls are in place. ■

About the Author

Ed Moyle | is a 15+ year veteran of information security as well as an industry-recognized thought leader, advisor, writer, and manager. Mr. Moyle is currently a faculty member at IANS, Senior Security Strategist with Savvis, and a founding partner of SecurityCurve. He can be contacted at *iatac@dtic.com.*

Trends in Academic Cybersecurity and IA Research Since 1996

by Karen Mercedes Goertzel

NOTE: An asterisk (*) next to a university's name indicates a National Security Agency/Department of Homeland Security-designated National Center of Academic Excellence in Information Assurance Research.

In the past 15 years, academia has contributed significantly to the advancement of information assurance and cybersecurity (CS/IA), but its specific contributions are often difficult to trace. Industry and non-academic non-profit research organizations take full credit for their advances. The MITRE Corporation, for example, showcases its "security automation" innovations, starting with its invention of Common Vulnerabilities and Exposures and Open Vulnerability Assessment Language. IBM, HP, Microsoft, McAfee, Symantec, and others are emphatic about advertising when their products originate in their own research labs. Government research organizations and labs often sponsor what is essentially academic research, which can downplay the leading roles academic researchers play.

These factors create a distorted perception that government, industry, and non-academic, non-profit research projects have been responsible for most of the CS/IA innovations of the past 15 years. The reality is that most, if not all, groundbreaking advances include content from academic researchers.

Academia's research contributions are also difficult to trace because institutions often engage in basic rather than applied research. Tracing the provenance of an actual CS/IA product or application to its basic research roots is seldom straightforward. Additionally, basic research that attempts to solve very hard problems may remain "basic" for years, even decades, with few if any practical implementations emerging; this is true of artificial immune systems, for example. While elements of artificial immunology have certainly appeared in anti-virus and anomaly-based intrusion detection systems, no one has implemented a practical, full-blown "artificial immune system" even after 25 years of research! [1]

Another example of a research area that remains in large part "basic" is quantum cryptography. The only commercially-viable application to date has been quantum key distribution (QKD), the two leading protocols for which emerged in part from academia: BB84 (1984), was invented by researchers at IBM Research and Université de Montréal, and E91 (1991) was invented at Oxford University. With the exception of Northwestern University's quantum, noise-protected data encryption technology, all other non-QKD research in quantum cryptography still defies practical implementation. Northwestern's quantum encryption technology was combined with BBN's QKD technology to produce a "quantum cryptographic data network" that runs over a 5.5-mile dedicated synchronous optical networking link between BBN headquarters and Harvard University.

It can also be difficult to trace whether a true innovation associated with a specific technology is its concept or its implementation (or both). For example, National Institute of Standards and Technology (NIST) scientists conceived the Advanced Encryption System (AES) as a symmetric-key encryption method that would avoid the proven vulnerabilities of Data Encryption Standard (DES) and DES-3. NIST then held a research competition to seek the best algorithm to implement AES. A decade later, NIST has repeated this approach with Secure Hash Algorithm (SHA)-3, a radically new approach to hashing that avoids earlier flaws. NIST is now in the final stages of the competition to find the optimal algorithm for implementing the new hash approach. So what are the true innovations—the AES and SHA-3 concepts developed by NIST, or the specific algorithms developed by academia and industry to prove those concepts? Either way, Joan Daemen's and Vincent Rijmen's Rijndael, the AES competition winner, is one of most significant cryptographic algorithms to emerge from academia (Katholiek Universiteit [K.U.] Leuven) in the past 15

years. The winning algorithm for SHA-3 may have the same distinction.

Origins of research innovations can also be obscured by "academic entrepreneurship," which allows these innovations to better transition into real-world use and takes several forms. [2] Research institutions and laboratories that are affiliated with universities are often formed to serve the needs of a particular industry or sector from which they receive funding. Some notable institutions of this type are Carnegie Mellon University (CMU*) CyLab and Software Engineering Institute, Johns Hopkins University* Advanced Physics Lab, and Purdue University* Center for Education and Research in Information Assurance and Security. [3] University business incubator programs and start-ups often allow academic researchers the opportunity to commercialize intellectual property (IP) they have developed, rather than licensing it to others. University-Industry Research Centers, such as those funded under the National Science Foundation Industry and University Cooperative Research Centers program, help innovations transition into practical applications. University patenting and licensing activities allow academic advances to transition into real-world use. Increased focus on industry grants and consulting contracts to individual academic researchers allow them to collaborate with industry experts and engineers, for example. Joint ventures and industry projects in computing and electronics engineering include one or more university partner(s) more often than projects in other research areas. These projects vary in duration, and such undertakings are often cost-shared with government (*e.g.*, under programs such as the NIST Advanced Technology Program). Finally, large university-based laboratories, such as the Stanford Center for Integrated Systems, are often funded wholly by industry consortia of tens, and even hundreds, of companies.

The increase in industry funding of academic research began in the early 1980s, at a time when government research funding dropped precipitously. At the same time, several government incentives and policies were initiated that promoted industry-academic partnerships under the Reagan Administration (*e.g.*, Research and Development [R&D] tax credits, the Bayh-Dole Act of 1980, relaxation of antitrust laws for R&D joint ventures); however, cultural barriers remain to such partnerships. Academics often consider industry emphasis on IP protection to be contrary to the openness needed for research. On the other side, industry sponsors often believe they own the resulted IP. Information and communications technology (ICT) companies in particular have a troubled history with academic researchers, accusing universities of unrealistic valuation and assertion of patent rights.

Disagreements over IP have been cited as the primary cause of the reversal of a three-decade-long trend towards increased industry investment in academic research in the U.S. "Largely as a result of the lack of federal funding for research, American universities have become extremely aggressive in their attempts to raise funding from large corporations, [which] have become so disheartened and disgusted with the situation, they are now working with foreign universities, especially the elite institutions in France, Russia, and China, which are more than willing to offer extremely favorable intellectual property terms." [4]

There are also growing ethical pressures on academic researchers to disassociate themselves from industry sponsorship. Where government funding of research was seen as benefiting society as a whole, industry funding is increasingly seen as benefiting only individual companies or business sectors. This attitude is particularly prevalent among researchers in the ICT realm, which generally supports open source information sharing. Due to industry's profit motives, many believe "commercially sponsored research is putting at risk the paramount value of higher education—disinterested inquiry" [5], while academic entrepreneurship raises "fundamental dilemmas about academic excellence, faculty autonomy, and the rationale for the university [to exist]." [6] Industry sponsorship is also accused of distorting research results, especially in the biomedical, agricultural, energy, and environmental domains; there, industry sponsorship is increasingly seen as inherently unethical.

These difficulties should not overshadow the significance of academia's CS/IA inventions and innovations of the past 15 years. Many of these have focused on further developing and refining earlier groundbreaking inventions from the late 1980s and early 1990s, such as RIPEMD-160 (K.U. Leuven), a stronger version of RIPEMD [7]; the improved version of the Domain Name System Security Extensions (Colorado State University was a contributor); and Datagram Transport Layer Security (Stanford University was the co-developer).

Academic research has also centered on developing techniques for proving the "breakability" of various popular (and not-so-popular) security protocols, cryptographic algorithms, and technologies, as a first step towards inventing new, less-vulnerable protocols, algorithms, and technologies. Here are some examples—

- The IP hash function collision attack for enabling covert channel analysis (University of California [UC]-Los Angeles);
- The cold boot attack for enabling data to be extracted directly from dynamic random access memory without operating system access and bypassing disk encryption (Princeton University*);

- Cryptanalysis of the Wired Equivalent Privacy and Cellular Message Encryption Algorithm (UC-Berkeley);
- Cracking of the A5/1 stream cipher used in Global System for Mobile cell phones (UC-Berkeley, University of Luxembourg, Weizmann Institute);
- Collision attacks against MD5, SHA-0, and SHA-1 (Shandong University, China);
- Cathode Ray Tube eavesdropping (University of Cambridge, England);
- Man-in-the-middle attack against chip-and-PIN-based smart-card credit/debit card systems whether online or offline (Cambridge); and
- Other cryptanalysis and side-channel attack techniques invented in academia since 1996: impossible differential cryptanalysis (University of Bergen, Norway), boomerang attack and rectangle attack (UC-Berkeley), and differential fault analysis (Weizmann Institute). In addition, at least one new mathematical underpinning for cryptanalysis emerged from academia, the forking lemma (École Normale Supérieure, Paris, France).

Researchers are always searching for better ways to transition their basic research into applied implementations and, ultimately, into common use. This is as true of academic researchers as it is to their counterparts in industry, government, and non-profit institutions. To this end, academic research continues to advance the state of the art of IA/CS with many noteworthy innovations and inventions, such as the following, which have emerged since 1996—

- Onion routing (Cambridge);
- Stack canary (Oregon Graduate Institute of Science & Technology, Ryerson Polytechnic);
- Completely Automated Public Turing Test to Tell Computers and Humans Apart technology (Weizmann Institute);
- Shibboleth (Internet2 Middleware Architecture Committee for Education, which includes numerous academic participants);
- Homomorphic encryption (Stanford);
- Secure coding standards for C/C++ and Java (CMU*);
- The first practical role-based access control model (George Mason University*);
- Viability and detection of hardware Trojans in integrated circuits (University of New Mexico, University of Connecticut*);
- Gordon-Loeb Model for Investing in Information Security (University of Maryland*);
- Gutmann Algorithm for secure deletion of data from memory (University of Auckland, New Zealand);
- First application of behavioral economics to the psychology of security (CMU*); and
- First application of econometrics to IA/CS (Stanford).

Because academic researchers are generally far more interested in the next research project than the last one, they often fail to keep track of what becomes of their innovations once those technologies and methodologies transition out of their labs. While it keeps academic research vital in its contribution to the advancement of the CS/IA state-of-the-art, this seeming lack of appreciation for their own research history does make determining whether, and how, that research sees the light of day in real-world applications and products. It may also explain why academic researchers appear to be less forthcoming than their non-academic counterparts about the ultimate fates of their research. They have already moved on to the next big challenge. ■

About the Author

Karen Mercedes Goertzel | is a Certified Information Systems Security Professional and leads Booz Allen's Information Security Research and Technology Intelligence Service. An expert in software assurance, ICT supply chain risk management, assured information sharing, and the insider threat to information systems, she has performed in-depth research and analysis for customers in the Department of Defense, the Intelligence Community, civil agencies, and industry in the U.S., U.K., NATO, Australia, and Canada. She was lead author/editor of Information Assurance Technology Analysis Center's State-of-the-Art Report on ICT Supply Chain Risk Management, the Insider Threat to Information Systems, and Software Assurance as well as a number of other IATAC information products and peer-reviewed journal articles and conference papers on these and other IA/CS topics. She can be contacted at *iatac@dtic.com*.

References

1. Los Alamos Lab physicists J. Doyne Farmer, Norman H. Packard, and Alan S. Perelson published their seminal "The Immune System, Adaptation, and Machine Learning" back in 1986, with key papers by other researchers following between 1990 and 1999.
2. Academic entrepreneurship is a much-studied phenomenon both within and outside the United States. A number of sources, three of which (Garnsey, Press, and Williams) were cited above, may prove useful for those wishing to understand the phenomenon. Please contact *iatac@dtic.mil* if you are interested in learning more about academic entrepreneurship.
3. UIUCs are not limited to the U.S. Examples abroad include the Information Security Institute at Queensland (Australia) Univ. of Technology, Japan's Research Center for Information Security, the Center for Information Security and Cryptography at Univ. of Hong Kong, and the Centre for Applied Cryptographic Research at the Univ. of Waterloo (Canada).
4. *Op. cit.*, Williams, Senate testimony.
5. *Op. cit.,* Press and Washburn, "The Kept University."
6. *Op. cit.,* Garnsey, "The Entrepreneurial University."
7. RIPEMD amplifies to Research and development in Advanced Communications technologies in Europe (RACE) Integrity Primitives Evaluation Message Digest.

Securing the Mobile Device…and its User

by Angela Orebaugh

Have you ever asked someone for the time and they pulled out their phone to get the answer? Today, smart phones have become as common as wristwatches in the 1900s. In fact, most of today's youth do not wear this old-fashioned form of mobile technology; they use their phones to tell time. Today's mobile technology includes handheld computing devices such as smart phones, personal digital assistants, tablet computers, electronic book readers, portable media players, and handheld gaming consoles. Mobile devices provide convenient access to information, entertainment, and communication by combining many functions into a single wireless device, including voice and video calling, texting, Web access, gaming, music, and movies. Some also include advanced features such as cameras, GPS, and the ability to pay for goods at point-of-sale terminals.

With such rich features and capabilities comes vulnerability. Imagine a scenario where an attacker has access to all of the data stored on your device, can follow your exact location and travel on a map, listen in on your cell phone conversations, and listen to conversations you have near your cell phone. This scenario is real and is happening to users across the world. Mobile malware and legitimate applications, such as FlexiSPY, provide an attacker with robust capabilities to access and monitor a mobile device without the victim's knowledge. [1] In addition to personal privacy violation, these types of applications also pose risks to business, politics, and even national security, depending on who is listening.

Challenges and Issues for Organizations

Due to the transformation in how users access and consume data with mobile devices, many organizations are now confronted with supporting the use and security of a number of mobile devices in the organization. Some organizations are even subscribing to the Bring Your Own Device operating model, which allows users to supply their own laptops and mobile devices for performing work and accessing company resources. Both organizations and users are faced with the fact that mobile devices often lack the security features available to personal computers. In some cases, this is due to slow market maturity for these products, and in other cases, the mobile device processing power does not support the overhead of traditional security tools such as firewalls and intrusion detection systems. Users also do not view their mobile devices as computers and often take more risks, such as opening attachments and downloading software. Mobile devices are susceptible to attacks similar to those targeted at personal computers, and criminals are taking advantage of vulnerabilities in mobile device operating systems and their users. The Norton Cybercrime Report states mobile vulnerabilities jumped 42% from 2009 to 2010 and 10% of adults have experienced mobile device-related cybercrime. [3]

What's Stored on Your Mobile Device?

- Photos
- E-mails (including deleted ones)
- Text messages (including deleted ones)
- Calls placed and received
- History of locations with geographic coordinates and timestamps
- Google maps and routes
- Web browsing history and browser cache
- Screenshots of applications in use
- User names
- Stored passwords
- Keystrokes. [2]

2011 became the year of mobile malware as mobile devices became a primary target for scammers and criminals. Mobile malware is increasing in volume and complexity with features such as botnet functionality and rootkits. Mobile devices are attractive to criminals because they hold a wealth of personal information including access to e-mail, social media, and bank accounts. Mobile malware attempts to steal personal data stored on the mobile device, access accounts using information stored on the device, and/or to use the features of the device for other cybercrime purposes.

Examples of Malware

- **Zitmo (Zeuz in the Mobile)**—Intercepts SMS messages to capture bank authentication codes;
- **DroidDream Botnet**—Steals phone identifier numbers;
- **Plankton—**Collects device ID and list of permissions and sends to a remote server;
- **Androidos_Nickispy.c—**Disguises itself as a Google+ app to capture instant messages, GPS location, call logs, and other sensitive data. Can automatically answer and record phone calls. Sends stolen data to remote site;
- **Pjapps/SteamyScr—**Turns the mobile device into a bot that an attacker can control;
- **Bgyoulu and GGTracker—**Sends messages to premium SMS services from the victim phone; and
- **SpitMo (Spyeye for Mobile)—**All incoming SMS messages are intercepted and transferred to the attacker's command-and-control server.

Main Attack Vectors

Mobile malware uses a number of different attack vectors to infect the mobile device. Some of the more common attack vectors include—

1. **Creating malware that looks like a legitimate application**—The most common attack on mobile devices is the result of repackaging. Cyber criminals add malicious code to a legitimate application and republish it to an application market or download site. [4] A variation of this is the upgrade attack, where an attacker first publishes a clean application, then later adds malicious code to an update of the application.
2. **Creating malware that executes from ads**—Some pop-up ads that are displayed on mobile applications will redirect the user to a site that downloads mobile malware.
3. **Creating malware that claims to be for security**—A traditional method of malware infection that tricks the user into installing a counterfeit version of security software is also making its way into mobile devices.
4. **Tricking the user into installing malware from an installation request originating from the victim's PC**—Some traditional malware that target PCs are now incorporating mobile components as well. For example, the Zeus Trojan that steals banking credentials on an infected PC has incorporated the Zitmo Trojan to capture SMS messages with banking authentication credentials sent to the infected mobile phone.

Most of these attack vectors are successful because users give applications permissions with no scrutiny.

Application Distribution

The method of mobile application distribution plays a significant role in the proliferation of mobile malware. Google and Apple have different philosophies and operational processes for vetting and distributing applications for their Android and iOS devices, respectively. Google allows flexibility for developers to create and distribute applications through a variety of channels including the Android Market and other third-party sites; however, Google does not vet the applications to ensure they are free of malware. Although this process allows increased flexibility, it comes with increased risk, as seen throughout 2011 with the increase of mobile malware for Androids. Thousands of free applications were found to have malware hidden in them. Once malicious applications are reported, Google removes access to them on the Android Market, but these applications still exist on third-party sites.

Malware is growing quickly with Androids, including some that steal personal information, send SMS messages to premium services, and record phone calls to upload to a remote server. [5] One example of Android malware is the DroidDream botnet that activates at night and steals phone International Mobile Equipment Identity (IMEI) numbers. Botnets are often sold in underground forums for spammers

and other cybercriminals. Cybercriminals can use the phone's IMEI number to make a clone of the phone and place calls, send text messages, and even order products, all of which will be charged to the victim's bill. After Google became aware of the malware, it flipped the "kill switch" that enables it to access Android phones without user permissions and delete the malicious software. About 260,000 Android users were infected with DroidDream. [6] Although it has been removed from the Android Market, DroidDream and its variants can still be found on third-party sites. [7]

Although some iOS malware exists, Apple has experienced less of an impact of malware due to its tightly controlled application distribution policy. Apple requires application developers to register and pay to obtain a signing certificate, making it easy to identify and prosecute authors of malware. Apple also tests every application that is submitted for publication to the App store for malware and policy violations. Apple also uses a code signing model that prevents tampering with published applications. Most iOS malware exists for devices that have been jailbroken, which allows the devices to run third-party software not vetted by Apple. Jailbreaking removes security settings and opens the device to malware and possible compromise.

Security Starts with the User

The main objectives for securing mobile devices are configuring security features and creating user awareness. The following recommendations include both security settings and user awareness—

- **Use strong passcodes**—Whether it is a swipe pattern, numeric PIN, or password to lock your device, make sure to use something that is difficult to guess. Avoid the most commonly used passcodes. [8] Enable the fingerprint lock option if supported by your device. Remember to also use strong passwords for applications that contain sensitive information. Some devices also have the ability to erase all data on the phone if the passcode is entered incorrectly after a certain number of attempts. Enable this feature and configure it to a reasonable number, such as 10 failed attempts.
- **Configure the screen lock**—Configure the screen lock to enable after a short period of inactivity, such as 1 to 5 minutes.
- **Disable Wi-Fi autoconnect**—Access the Internet using the service provider's network (*e.g.*, 3G) or a secure wi-fi network. Unsecured wireless networks may expose sensitive data to attackers on that network. Do not use a public Wi-Fi, even if secure, for financial transactions or other personal transactions.
- **Scrutinize links**—Do not click suspicious or unknown links regardless of the sender.
- **Scrutinize text messages**—Do not respond to text messages from unknown sources or strange requests from known sources.
- **Download applications from trusted sources**—Only download applications from trusted sources and distribution channels.
- **Understand permissions**—Make sure you understand the permissions an application is requesting before accepting. If the application is asking for permission to access something that seems unusual for its purpose, such as access to your location or contacts, ensure the application is legitimate and free of malware before granting permissions.
- **Install theft location applications**—There are applications for some devices that allow the device to be located and certain features managed remotely. For example, Apple's Find My iPhone and Find My iPad applications are used to locate a lost device. They include features to remotely set or enable the passcode lock and remotely wipe the device.
- **Do not jailbreak the device**—Jailbreaking a device removes limitations and security parameters and exposes the device to increased security threats.
- **Make sure the device OS is up to date**—Promptly apply updates as they are released for your device.
- **Think about the type of data stored on your device**—Whenever possible, do not store sensitive data on mobile devices. If sensitive data is stored on your device, make sure the data is encrypted.
- **Use security software and keep it up to date**—A number of security vendors have developed applications to add third-party mobile device security, including Trend Micro, ESET, McAfee, Symantec, and Webroot. Install a security application appropriate for your device and usage.

Mobile Device Attack Scenario

A security researcher at the 2010 Defcon conference launched a man-in-the-middle attack on cell phones, allowing him to eavesdrop on conversations. He built a fake cell phone tower for $1,500 and used it to stealthily intercept phone calls and pass them on to a real tower. This research only works on GSM-based networks but serves as a proof-of-concept of the ease of interception of cell phone communications. [9]

There are still many organizations that are not yet addressing the proliferation of mobile device usage.

Enterprise Mobile Device Security

Mobile devices are changing the way organizations manage security. Many information technology departments

are now treating users as shared owners of the end-user technology, giving them flexibility to use their own personal devices, but also holding them responsible for proper device usage and security; however, there are still many organizations that are not yet addressing the proliferation of mobile device usage. "More than one out of five organizations do not have a security policy governing the use of personal mobile devices at work, even though two out of three said they allow personal mobile devices on the corporate network," according to a survey by Courion. [10] The survey also stated that "one in 10 organizations has had a data breach following the loss of a personal mobile device." Organizations must implement a mobile device policy to define, assess, and enforce access and also to outline incident response procedures. Redspin provides an example Mobile Device Security Policy available for download at *http://www.redspin.com/docs/WP_Redspin_Mobile_Device_Security_Policy.pdf.*

Some additional recommendations for mobile device security for organizations include—

- Centralize mobile device administration to enforce and report on security policies;
- Strongly enforce security policies, such as mandating the use of strong passcodes;
- Enforce mobile device security applications to protect against malicious applications, spyware, and other attacks;
- Use SSL VPN clients to require authentication and protect data in transit;
- Centralize location and remote lock, wipe, backup, and restore capabilities for lost and stolen devices;
- Use software to monitor device activity for data leakage and inappropriate use; and
- Incorporate planned internal phishing exercises to measure security awareness and educate users who are falling for these attacks.

Mobile Device Pioneers in Government

A number of government agencies are adopting enterprise strategies for mobile devices. The state of West Virginia uses software from Good Technology that enables users to securely access business-related information from any device, including personal mobile devices. State personnel can also request iPhones, iPads, and Android-based smart phones for business and personal use. The Good Technology software enables secure calls and messaging by segregating business and personal information in "containers" with individual encryption and policy controls. [11] The United States Department of Agriculture (USDA) is testing the ability to secure personal mobile devices using technologies such as a virtual desktop infrastructure that mimics a secure PC environment. The USDA maintains an inventory of several thousand government-issued devices such as iPads, iPhones, and other smart phones. They are also creating mobile device management standards and policies for use by all government operations. [12] Other government agencies supporting mobile devices include the State Department, the General Services Administration, the Department of Interior, and the Department of Defense.

Many health-care providers are also embracing mobile devices. Just 1 year after the iPad was released, 30% of the U.S. physicians began using it and an additional 28% plan to purchase an iPad within the next 6 months. [13] Doctors at the Veterans Affairs are also using smart phones and tablets to access patient records. [14]

The rapid adoption of mobile devices has created a rich opportunity for cybercriminals.

The Mobile Future

The rapid adoption of mobile devices has created a rich opportunity for cybercriminals. As criminals create malware and other attacks on mobile devices, it is likely that they will become the primary target for cybercrime and a key element of financial crime in the future. With an increasing number of users bringing mobile devices into the enterprise, we will see more cross-platform attacks that target enterprise assets. Mobile devices will become the stepping-stones to protected information in the cloud and other data stores. As mobile device security evolves, it is important to educate users, enable available security settings, and continue to stay on the forefront of attack methods and countermeasures. ■

About the Author

Angela Orebaugh | is a technologist, researcher, and cybersecurity executive, who is passionate about helping clients embrace tomorrow's technology today. Ms. Orebaugh was recently selected as Booz Allen Hamilton's first and currently only Cyber Fellow, a distinction reserved for an elite group of the firm's most noted authorities. She evangelizes social media and mobile technologies by highlighting the powerful ways in which these technologies are changing business, communications, and information sharing. Ms. Orebaugh is also the Information Assurance Technology Analysis Center Director of Research and Academic Integration. She is an international author and invited speaker for technology and security events. Follow her on

▷ ▷ *continued on page 33*

Security Through Understanding…and Emulating…the Advanced Persistent Threat

by Ronald Ritchey and Karen Mercedes Goertzel

The sophistication of the threat is increasing at least as fast, if not faster, than that of the systems and networks targeted by it. The instigators of today's advanced persistent threats (APTs) are ingenious, creative, well-resourced, and patient. In many ways, they are on the leading edge of system and software engineering, in terms of their ability to design and implement complex, sophisticated distributed systems of cooperative software agents that are elegantly minimalistic yet highly reliable, survivable, and effective.

Understanding how APTs operate and how they are engineered can provide many clues into how the systems and networks targeted by them could be re-engineered so that our dependency on a failing security paradigm—protect-detect-react-recover, which can never hope to keep up with the rapidly evolving, increasing capabilities of APTs—can be replaced with a commitment to engineering systems and networks capable of withstanding, surviving, and better yet avoiding the effects of such threats.

An Advanced Persistent Threat in the Real World

Our story begins as many APT cases begin, with a small incident that might have gone unnoticed. The employee of a small firm worked from home a few days a week. He lived in a town with an unreliable power grid, which meant he often experienced fluctuations, spikes, sags, and even outages, especially during storms. During one such power anomaly, his computer locked up, and he had to reboot. When the computer came back on, the employee noticed a set of files on his desktop that were not there before. These files were all compressed RAR files 650K bytes in size. [1] Becoming suspicious, he reported the incident to his company's information security team.

Most APT attacks can only be found through this kind of *ad hoc* discovery because most methods used by APT attackers are undetectable by popular intrusion detection and security monitoring systems and tools. These systems and tools compare incoming network traffic and resulting host activity against "signatures"—machine-readable encapsulations of patterns of network input and host activity observed during previous attacks—stored in the systems'/tools' libraries. If a new input or host behavior matches one of the stored signatures, the new input/behavior will be flagged as suspicious or indicative of a likely attack. The system/tool will then issue an alert to the administrator, block further traffic on the network port over that the input was received, terminate suspicious network sessions or host process, or perform some combination of these and/or other responses.

While signature-based tools, including signature-based anti-virus scanners, are quite good at detecting known patterns that have been replicated thousands of times across the Internet, they cannot recognize patterns that contain even minor deviations from those encapsulated in their stored signatures. For this reason, signature-based tools do not help much against APTs because APT attacks include unique exploits tailored for their specific targets. Though APT attackers must study and become familiar with their intended targets to tailor effective attacks against those targets, unfortunately for those who wish to defend against APTs, these "reconnaissance" and attack-crafting activities do not actually require great amounts of time or resources, just ingenuity and dedication on the attackers' part.

Once the employee's company received the report of the suspicious RAR files, the information security team's analysts immediately suspected that the employee's computer had been the target of an attack. The team began a painstaking forensic investigation that started with gathering and combing through network, file system, firewall logs, e-mail records, and other data to piece together the most likely trail of events that caused those RAR files to

▷ ▷ *continued on page 34*

CSIAC Prepares Organizations to Tackle the Newest Battlespace—Cyberspace

by Christopher Zember

On April 19, 1775, shots rang out in Lexington and Concord. In the months that followed, countless battles took place between British troops and a ragtag group of colonial patriots. The British, with their well-financed government and professional military, had almost every advantage over the rebellious colonials. For the next 8 years, David squared off against Goliath in a fight for freedom and over a land that would soon become America.

Fast-forward nearly 200 years, and it is clear that the United States has developed perpetual advances and unquestioned superiority in the traditional fighting domains of land, sea, and air. Driven by innovation and collaboration, and forged in battle, advances in U.S. defense have changed the course of history; however, despite our near mastery of traditional battlespaces, a new fighting domain has emerged. Today, experts predict that our nation's toughest battles will take place not in one of the traditional domains, but rather in the emerging domain of cyberspace.

While still misunderstood to many people, cybersecurity is an important topic stretching beyond our national security challenges and into all facets of our ever-growing digital lives.

In June 2010, in response to the ever growing cyber threat, Secretary of Defense Robert Gates announced the launch of the U.S. Cyber Command (USCYBERCOM), which operates as a subordinate unified command under the U.S. Strategic Command (USTRATCOM), fusing the Department of Defense's (DoD's) full spectrum of cyberspace operations. From planning, coordinating, integrating, synchronizing, and conducting activities, to leading day-to-day defense and protection of DoD information networks, USCYBERCOM coordinates DoD operations and provides support to military missions. Despite USCYBERCOM's strong track record and early successes, the danger of cyberwarfare remains an imminent threat.

In a June 2011 address, President Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity." While still misunderstood to many people, cybersecurity is an important topic stretching beyond our national security challenges and into all facets of our ever-growing digital lives.

In the age of Facebook and Twitter, all organizations are forced to re-evaluate the fine line between sharing and securing their information.

In the age of Facebook and Twitter, all organizations are forced to re-evaluate the fine line between sharing and securing their information. This is especially true for government organizations, and the challenge only intensifies for large agencies working with sensitive information. The DoD grapples with maintaining this complex and often fluid dichotomy. While the line between sharing and securing information is often unclear, the need for a Center of Excellence containing best practices and expertise on cyber-related threats is unquestionable.

▷ ▷ *continued on page 28*

Thank you for over

13 Years

of sharing Information Assurance and Cybersecurity information with us!

~ The IATAC Team

IATAC Homepage

Technical Inquiries

Twitter

Wikipedia

Newsletter

Reports

IATAC
INFORMATION ASSURANCE & CYBERSECURITY

This is a representative sampling of events

96

President Clinton signs the Health Insurance Portability and Accountability Act (HIPAA).

The Nokia 9000 Communicator becomes the world's first cell phone with Internet connectivity.

DoD issues its Directive 5200.1, "DoD Information Security Program" (with a supporting Regulation to follow in 1997).

97

The ELIGIBLE RECEIVER information warfare exercise demonstrates DoD's vulnerability to networks penetrations and associated mission disruptions.

The National Information Assurance Partnership (NIAP) is established.

DoD Instruction (DoDI) 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)" is issued.

The Defense Information Systems Agency (DISA) stands up its IA Support Environment (IASE).

The G8 holds the first High-Tech Crime Subgroup meeting.

98

The Defense-wide Information Assurance Program (DIAP) is established under the DoD Chief Information Officer.

Hackers launch Operation SOLAR SUNRISE, hacking into Air Force, Navy, and Marine Corps unclassified networks, stealing hundreds of passwords, and using them to access the Global Transportation System, the Defense Finance System, DoD medical, personnel, e-mail systems, and computer networks at Lawrence Livermore National Lab.

Canada, France, Germany, the United Kingdom (UK), and the U.S. sign the Common Criteria Mutual Recognition Arrangement (MRA).

President Clinton signs Presidential Decision Directive 63 (PDD 63) "Critical Infrastructure Protection."

Google is founded.

DoD establishes the Joint Task Force Computer Network Defense (JTF-CND).

The Defense Technical Information Center (DTIC) formally establishes IATAC.

99

President Clinton announces a $1.46 billion initiative to improve government computer security.

The Melissa e-mail virus infects computers worldwide, causing an estimated $80 million in damage.

Gramm-Leach-Bliley passed establishing governance for personally identifiable information.

15-year old Jonathan James, (a.k.a. cOmrade) hacks into the Defense Threat Reduction Agency (DTRA) computer network, various computers at DoD, and computers at the National Aeronautic and Space Agency (NASA). When later charged and convicted, James becomes the first juvenile ever sentenced to prison (6 months) for computer crimes.

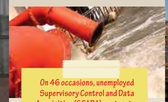
Canada's Research in Motion releases the first Blackberry mobile e-mail device.

The MITRE Corporation launches its Common Vulnerability Enumeration (CVE) initiative.

00

January 1 comes and goes. Computers keep running. Preparations are successful.

The White House issues the first-ever National Plan for Information Systems Protection.



On 46 occasions, unemployed Supervisory Control and Data Acquisition (SCADA) contractor, Vitek Boden, uses stolen radio equipment, laptop, and software to hack into the Maroochy Shire (Queensland, Australia) water authority's SCADA system and release millions of gallons of raw sewage into local rivers, parks, and hotel grounds.

Trek Technology and IBM start selling the world's first commercial Universal Serial Bus (USB) flash drives.

The "I Love You" (a.k.a. "LoveBug") e-mail virus spreads worldwide, costing more than $10 billion dollars to eradicate.

01

UK hacker Gary McKinnon begins a year-long cyberattack on nearly 100 U.S. government computers and networks.

11 September: the United States transforms; cybersecurity becomes more critical

The Council of Europe Convention on Cybercrime is signed—the first and only international treaty on Internet-based crimes (the U.S. is a signatory).

Congress enacts the USA PATRIOT Act, which includes a mandate for a nationwide network of Electronic Crimes Task Forces (ECTFs).

NIST publishes FIPS 140-2 and FIPS PUB 197, the latter designating the Rijndael algorithm as the Advanced Encryption Standard (AES) that will replace 3DES as the standard federal government encryption algorithm.

02

Sarbanes-Oxley passed ensuring companies have adequate information security protections for financial information.

DoD issues Directive 8500.1, "Information Assurance."

The Federal Information Security Management Act (FISMA) is enacted as Title III of the E-Government Act.

Anonymous hackers launch a massive 1-hour distributed denial of service attack against 9 of the Internet's 13 Domain Name Service (DNS) root domain servers.

OWASP publishes its first "Top 10" list of Web application vulnerabilities.

Microsoft

Microsoft launches its Trustworthy Computing initiative.

03

The White House publishes the *National Strategy to Secure Cyberspace.*

DoD issues Instruction 8500.2, "Information Assurance (IA) Implementation."

President Bush issues Homeland Security Presidential Directive-7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection."

Within 10 minutes of its release, the SQL Slammer (a.k.a. Sapphire) worm infects 75,000 computer systems, making it the fastest-spreading computer worm in history. Within 3 hours, it infects hundreds of thousands of computers, forces most of South Korea and Japan offline, disrupts phone service in Finland, and brings online bank and credit card services in the U.S. to a near-standstill.

DHS establishes the US-CERT.

The Trusted Computing Group forms to define Trusted Processor Module (TPM) standards.

04

PCI Security Standards Council

The Payment Card Industry Security Standards Council forms to align security programs of Visa, MasterCard, American Express, Discover, and JDB into a single Payment Card Industry Data Security Standard (PCI-DSS).

The MD5 hash is proven insecure by researchers using a birthday attack.

facebook

Facebook is founded.

DoD issues Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management."

id Quantique begins selling the first commercial quantum key distribution system.

05

The President's Information Technology Advisory Committee (PITAC) releases *Cyber Security: A Crisis of Prioritization.*

NIST publishes SP 800-53, *Recommended Security Controls for Federal Information Systems.*

ISO/IEC 27001, *Information Security Management Systems—Specification with guidance for use,* is adopted as an international standard.

A massive computer breach at a payment processing company exposes more than 34 million Visa and MasterCard account records.

Using publicly-available tools, FBI "white hats" crack Wired Equivalent Privacy (WEP).

DHS and NIST stand up the National Vulnerability Database (NVD).

06

DHS's Cyber Storm exercise simulates a large-scale attack on U.S. critical digital infrastructure, revealing that U.S. resources allocated to cybersecurity would be "overwhelmed in a real attack."

The International Multilateral Partnership Against Cyber-Terrorism (IMPACT) is established.

Advanced Persistent Threat "Operation Shady RAT" is launched, potentially from China, against 70+ organizations in 14 countries. It continues to this day.

IMPACT, the International Multilateral Partnership Against Cyber-Terrorism (later changed to Cyber Threats), is established.

NIST publishes FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems.*

07

A series of cyber attacks on U.S. government computers results in the loss of 10-20 terabytes of data—more than the total holdings of the Library of Congress—while an extended cyber attack on its computers forces the Pentagon to temporarily disconnect NIPRNET from the Internet.

FBI Operation Bot Roast and Operation Bot Roast II reveal more than two million bot-infected zombie computers on the Internet.

Following Estonia's decision to move a Soviet World War II Memorial, Web sites of Estonian banks, media outlets, government, and political organizations are attacked through a coordinated attack. This incident sparks international discussion as to whether or not cyber attacks constituted "clear military action."

DISA, NSA, and NIST establish the Information Security Automation Program, with participation by OSD and DHS.

DoD Instruction 8500.01, "Defense IA Certification and Accreditation Process (DIACAP)" is finalized.

08

President Bush issues National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) directing the establishment of the Comprehensive National Cybersecurity Initiative (CNCI).

cloud security alliance

The Cloud Security Alliance is formed.

NATO opens its Cooperative Cyber Defence Centre of Excellence opens, and declares its first Cyber Coalition exercise a success.

09

President Obama orders a White House Cyberspace Policy Review.

DoD stands up the U.S. Cyber Command (USCYBERCOM).

The Conficker botnet worm hits its peak, infiltrating millions of PCs worldwide including "secure" government PCs.

Google detects "Operation Aurora," a "highly sophisticated, coordinated, and targeted attack on its corporate infrastructure originating from China.

10

Wikileaks

The Senate Committee on Homeland Security and Governmental Affairs passes the Cybersecurity Act of 2010 by voice vote, but the measure is not taken up by the full Senate.

An intelligence analyst, Bradley Manning, is arrested in Iraq for copying classified data from SIPRNet, including 250,000 diplomatic cables and video footage of various U.S. airstrikes in Iraq and Afghanistan, and posting them on WikiLeaks.

The Stuxnet worm emerges as the first malware to target a specific model of SCADA system—the Siemens WinCC, known to be used at Iran's Natanz and Dushehr uranium enrichment facilities.

The U.S. joins discussions with 14 other countries on a proposed UN cyber arms control treaty.

11

A new "antisec" hackivist group, LulzSec, launches a 50-day hacking spree against Web sites worldwide, including U.S. government sites. LulzSec steals credit card data from 70 million user accounts on the Sony Playstation and Qriocity sites. The group allegedly retires, though more LulzSec-credited attacks followed.

The UK government launches a public inquiry into the 5 years old *News of the World* phone hacking scandal.

The Department of Energy releases its *Roadmap to Achieve Energy Delivery Systems Cybersecurity.*

VIRTUAL IAC

▷ continued from page 25

CSIAC will be a consolidation of three existing legacy IACs: the Data and Analysis Center for Software (DACS), the Information Assurance Technology Analysis Center (IATAC), and the Modeling and Simulation Information Analysis Center (MSIAC).

Enter the Cyber Security and Information Systems Information Analysis Center (CSIAC), the newest DoD Information Analysis Center (IAC) focused on leveraging best practices and expertise from industry, government, and academia on these and other cyber-related threats. Established to solve the government's toughest scientific and technical challenges, CSIAC will be a consolidation of three existing legacy IACs: the Data and Analysis Center for Software (DACS), the Information Assurance Technology Analysis Center (IATAC), and the Modeling and Simulation Information Analysis Center (MSIAC). CSIAC will maintain and expand the knowledge bases of the legacy IACs, which include over 27,000 holdings of physical scientific and technical information and a vast online knowledge base. These include information surrounding emerging technologies in system vulnerabilities, information assurance, effective defenses against information warfare attacks, software technology, software engineering, and modeling and simulation. CSIAC will also expand into other areas of strategic importance and closely monitor new technologies emerging within the discipline.

Organizations looking to take advantage of CSIAC will be able to do so starting in early 2012, the planned award date for the CSIAC contract. The legacy IACs (*i.e.*, DACS, IATAC, and MSIAC) will then begin a 90-day transition period as CSIAC is established. Once fully operational, CSIAC will begin offering free technical inquiry research, as well as more in-depth, cost-structured services, to customer agencies across the government. CSIAC will maintain expertise in five cybersecurity and information systems domain areas and grow that knowledge base in areas of strategic importance. Organizations will now have a one-stop shop for pertinent information within this growing field. CSIAC will also serve as the IAC foundation for extended research. Government agencies may order extended research from CSIAC 's companion task order contract, SNIM (Software, Networks, Information, Modeling & Simulation), awarded in May 2010 *(http://iac.dtic.mil/snim.html)*.

Over our 235-year history, the United States has evolved and grown into what some call "the last great superpower." Our innovation, collaboration, and determination have allowed us to meet the ever-changing fighting domains. As the nation continues to evolve, so does the IAC, forever ensuring a solid foundation of knowledge and intellectual capital ready to meet our nation's current and future needs. As the battle space continues shifting into the digital world, our nation can rest assured that there is a central resource where agencies can turn as they prepare to battle in cyberspace. ■

Our innovation, collaboration, and determination have allowed us to meet the ever-changing fighting domains. As the nation continues to evolve, so does the IAC, forever ensuring a solid foundation of knowledge and intellectual capital ready to meet our nation's current and future needs.

About the Author

Christopher Zember | is the Deputy Director of the DoD IACs, under oversight of the Assistant Secretary of Defense for Research and Engineering. He is responsible for operational management and policy guidance for 10 IACs, comprising a $14 billion portfolio in technical research and analysis. Prior to his current position, Mr. Zember led the Strategy and Operations practice for a small consulting firm and also served as a member of the core research team in a congressionally-chartered effort to rewrite the National Security Act. Mr. Zember holds a B.A. in English from Harding University and a M.P.A. from American University.

Cyberlaw's Evolution Over the Past 20 Years

by Rick Aldrich

"The law must be stable, but it must not stand still." Roscoe Pound (1870-1964)

Many claim the law has not kept up with technology, and with the pace of technological change over the past couple of decades, this may be true, but the law has certainly not stood still. This article highlights a few of the more significant and curious changes in the law over the last 20 years or so.

The Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) was an expansive piece of legislation, passed in 1986, that extended the Federal Wiretap Act (FWA), which previously only covered oral and wire (telephone) communications, to also cover electronic communications. [1] It also added provisions governing stored communications [2], pen register traps and traces [3], and National Security Letters. [4] What few people may have realized is that the FWA offered very few specific exceptions to the general prohibition against intercepting communications. The Justice Department opined that law enforcement agents and counterintelligence agents could not even intercept hackers breaking into their own agency's networks in most cases. This was because the consent exception, which would have seemed to be the most obvious choice, required the consent of "a party to the communication." [5] The rationale was that hackers were not communicating with anyone but the computer. They did, however, often attempt to hack into systems in the middle of the night when they hoped no one was using the computer. Since the hacker was the only party to the communication, the only way to use this exception was *via* the consent of the hacker. For that reason, the Department of Defense (DoD) and other government agencies adopted a policy of bannering computer ports where hackers might enter. The banners essentially stated that proceeding beyond that point constituted consent to monitoring. Unfortunately, computers have 65,536 ports and many cannot effectively be bannered. A human might not necessarily even see those computer ports that could be bannered because of the way certain exploits were accomplished. Some thought they could just banner the ports that were open, but hackers would drop off exploits that would open other ports and enter through them. Additionally, some wondered how effective the consent was when an increasing number of hackers were coming from abroad and may not have even understood English. To overcome all of this, Congress amended the FWA, *via* the USA PATRIOT Act, to create a new exception for computer trespassers. The exception had four prerequisites [6], but finally provided law enforcement and counterintelligence agents with a legal basis for tracking trespassers that did not rely on the uncertainty of bannered ports or require the lengthy process of obtaining a wiretap order or Foreign Intelligence Surveillance Act (FISA) court order.

Legislatures have a propensity to write specific laws to address perceived problems with a specific technology. Unfortunately, this requires the laws to change as rapidly as the technology does. Since that generally does not happen, the results can be curious. The Stored Communications Act required different procedures depending on whether the seizure was of a wire or electronic communication. As the technologies for wire and electronic communications merged, problems emerged. For example, the law required only a search warrant to seize stored electronic communications (e-mail), but required a wiretap order to seize stored wire communications (voicemail). [8] From this, the courts determined that a voice attachment to an e-mail required a wiretap order. This greatly complicated seeking the appropriate legal authority to seize e-mail, because one could never be sure whether any of the e-mails might contain a voice attachment, in which case a wiretap order would be necessary. A change in the law permitted both to be obtained by use of a search warrant. [9]

Another problem arose when technology evolved to permit cable companies to offer services that previously only Internet service providers (ISPs) offered. The Cable Act, which was enacted in 1984, placed high burdens on governmental entities when obtaining information from a cable company. It required the subscriber be notified and afforded the opportunity to contest the order in court, and required the government meet a "clear and convincing" standard of proof that the customer was reasonably suspected of engaging in criminal activity. This was dramatically different from the procedures necessary to get the same information from a non-cable ISP, which required no notice to the subscriber, no opportunity for the subscriber to contest the order, and only showing that there were "reasonable grounds" because the records sought were relevant and material to an ongoing investigation. This dramatic discrepancy, based solely on what type of entity provided the Internet services, was changed in 2001 to make accessing Internet records, whether under the FWA, ECPA, or the Pen Trap and Trace Statute, the same for all. [10]

The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) is the federal government's preeminent anti-hacking statute. [11] An important term that defines the scope of several key provisions in the statute is the rubric "protected computer." It started out as "federal interest computer," which had a narrower scope. Then in 1994, Congress changed it to "computer used in interstate commerce or communications," but in doing so inadvertently excluded the protection of U.S. government computers and financial institutions' computers that were not used in interstate commerce; therefore, the law was amended again in 1996 to define "protected computer" to include all of the above. [12] In 2001, the term was expanded to explicitly extend extraterritorially by including computers used in foreign commerce. [13] Then in 2008, the term was further expanded to cover any computer that was used in or affected interstate or foreign commerce, ensuring coverage of even those computers used solely intrastate, as long as they affected interstate or foreign commerce, presumably encompassing all computers that can connect to the Internet.

Currently, one of the more controversial provisions of the CFAA is a provision that makes certain accesses to protected computers illegal "without authorization" or in excess of authorization. The "without authorization" terminology had traditionally applied to external hackers. Over time, however, it is applied to anyone who violates a term of use in a user agreement, or even to employees who use their company computer to engage in acts "disloyal" to the company. This led to the famous case of Lori Drew. [14] Lori Drew was the mother of a teenage girl who decided to "mess with" one of her daughter's ex-friends, 13-year old Megan Meier, by posing, as an attractive 16-year old boy under the name "Josh Evans" *via* MySpace. After developing a strong bond between Josh and Megan *via* MySpace, the mother (*via* Josh) harshly suggested that "the world would be a better place without you," resulting in Megan's suicide. Ms. Drew was charged with a violation of 18 U.S.C. 1030(a)(2)(C), which punishes intentionally accessing a computer "without authorization" or in excess of authorized access, and thereby obtaining information from any protected computer. The theory was that Ms. Drew violated MySpace's terms of service, which required all registration information be truthful and accurate, and therefore her access to MySpace's computers, which were "protected computers" as defined above, was unauthorized. The jury convicted Ms. Drew on three counts, but the judge set aside the verdict on the Defense's motion, holding that interpreting the statute in the manner supporting the government charges rendered it unconstitutionally vague because it left too much discretion to law enforcement officers and failed to adequately place citizens on notice as to what was criminal. To rule otherwise would have left it up to each company's discretion to determine who was and was not in violation of the company's terms of use, and therefore arguably committing a felony. MySpace had many other terms of use that would have made virtually everyone a felon. [15] At the time this article was submitted for publication, Congress was considering amending the CFAA to address the above-noted overbreadth problem.

The Lori Drew case was a criminal case, but a 1994 change to the CFAA permitted civil actions under its terms also. Recently, there have been a flurry of cases by companies alleging CFAA violations by employees who engage in the use of corporate computers that is "disloyal" to the company (usually sharing proprietary information with competitors) or in violation of the company's terms of use. These cases have met with mixed success in the courts, creating significant uncertainty in this area of the law.

Stretching the law even further, Sony recently sued George Hotz under the CFAA claiming that his "jailbreaking" of his Sony PlayStation 3 constituted an "unauthorized access" of his own computer based on the terms in the manual that accompanied the computer and the terms of the PlayStation Network account. While admittedly Sony may have had valid claims under the Digital Millennium Copyright Act, under a contract claim, or other causes of action (which were also included in the suit), it seems that contorting the CFAA to support a federal lawsuit for unauthorized access to one's own computer goes too far. Such are the problems, however, with loosely defined statutory terms and rapidly changing technology. Sony ended up settling the case, so we do not have a clear answer

on how the courts would ultimately have decided this issue.

The Pen Register Trap and Trace statute

The Pen/Trap and Trace statute originally only applied to obtaining the numbers dialed when making an outgoing call or trapping the numbers dialed on an incoming call. [16] In 2001, with the USA PATRIOT Act, Congress expanded the scope to include "routing, addressing, or signaling information" for electronic communications as well. [17] This was a boon to government investigators because the standard for obtaining a pen/trap order were dramatically lower than that required to intercept or obtain stored communications, yet could provide significant assistance in investigating computer crimes.

Now the law is being expanded further to obtain cell-site location data. Cell phones send out signals periodically to connect to towers to obtain or retain reception. Oftentimes such signals are received by several towers, and using triangulation techniques, one can ascertain the approximate location of the cell phone (with a high degree of accuracy in dense urban areas, less so in rural areas with fewer towers that are further apart). Because a high percentage of Americans now carry a cell phone with them virtually everywhere, it has become increasingly tantalizing to investigators, to obtain that information to prospectively track suspects or to retrospectively place them at the scene of the crime. Cell-site data falls within the realm of "routing, addressing, or signaling information," but the Communications Assistance for Law Enforcement Act of 1994 precludes the government from relying "solely" on the authority of the Pen/Trap statute to obtain such data on subscribers, so prosecutors have developed a hybrid theory, which pairs that authority with the authority of a 2703(d) order, so named for the statutory section under the CFAA that authorizes it. [18] This hybrid theory has met with mixed success, with several courts upholding it and several others, claiming that a search warrant is needed. The prospect that prosecutors could track the movements of Americans 24/7 by meeting only a very low legal threshold suggests George Orwell's 1984 to some, but to others one's movements in public places should enjoy no reasonable expectation of privacy. The Supreme Court addressed a very similar issue in November 2011 in the case United States v. Jones. [19] The government attached a small GPS tracking device to Jones' wife's car and obtained data on his exact whereabouts every 10 seconds for almost a month, without a warrant, ultimately using that data to convict him on drug charges. The decision in that case, expected in early 2012, is likely to send a strong signal as to how the court would rule in obtaining cell-site location data without a warrant as well.

Other Evolutions in Cyberlaw

The use of social media has grown dramatically over the past few years with Facebook now hosting over 800 million users. [20] The DoD has embraced the new technology with the Directive-Type Memorandum that directs its unclassified network be "configured to provide access to Internet-based capabilities across all DoD Components." [21] This, however, has raised concerns for some military commanders in the Iraq and Afghanistan theaters, who fear their troops may unwittingly reveal sensitive operational information with posts such as, "Sorry honey, homecoming delayed. We're making a strike near Kandahar this Saturday." To avoid this operations security violation, some commanders have ordered members of their unit to provide their social media account names to make monitoring such communications easier. Commanders who visit the accounts of military members who have properly set their privacy settings will likely only see a message indicating that the individual only shares his personal information with his Friends. This raises the rather novel legal question of whether a commander can order his subordinates to be his Friend; however, even if the commander issues such an order, subordinates could easily keep the commander in the dark still by placing the commander on a Friend list that filters what the commander could see. Some communities are asking for complete access by requiring job applicants provide their social media account names and passwords. Maryland's Department of Public Safety and Corrections suspended such a policy in February of 2011 after the American Civil Liberties Union publicized the policy. [22]

Government workers with certain security clearances are generally required to report "close, continuing personal association" with foreign nationals. [23] With the proliferation of social media, many now construe that requirement to extend to Facebook Friends. Admittedly, some accept Facebook Friends even if they do not know the individual well (or at all), which may not meet the reporting threshold of a "close, continuing personal association." Nevertheless, failure to report such Facebook Friends will likely only complicate one's security investigation, especially if the investigator is not well acquainted with the technology and wonders why one has failed to report a foreign national that is characterized as a Friend.

Another new legal issue to emerge from the growth of social media is whether a supervisor's unfriending on Facebook of a subordinate would constitute an adverse personnel action, triggering due process rights. Interestingly, the National Aeronautics and Space Administration (NASA) set up its own social media site, Spacebook, somewhat differently to avoid this issue. [24]

Virtual worlds, such as Second Life, Maple Story, and others, permit one's avatar to do virtually anything an individual could do in the real world;

therefore, people buy and sell virtual real estate, get married and divorced, travel to distant virtual lands, *etc.* Second Life has become so popular that some countries have even established virtual embassies in Second Life, prompting the question, "Should a person with a security clearance be required to report visits to virtual embassies in Second Life, just as one is required to report visits to embassies in the real world?" Currently, there appears to be mixed opinions on this issue from various security offices, with some presumably unaware that such embassies even exist.

Another case involving virtual worlds related to a Japanese woman whose avatar was involved in a messy divorce from her virtual husband. She was so upset she decided to kill his avatar. Does such a killing constitute a crime? Most would laugh and deride the very question, but in fact she was charged—not with murder but with a computer hacking offense. It turns out in the virtual world in which they divorced, Maple Story, there was no means of killing another avatar; therefore, the distraught divorced avatar relied on her real-world persona to hack into the computer of her virtual ex-husband and destroy the bits that supported his digital persona in Maple Story, effectively "killing him." For this real-world offense, she was charged and could receive a maximum penalty of 2 years confinement and the equivalent of about a $5,000 fine.

In a virtual game world, RuneScape, two Dutch teens who were unable to earn a much sought virtual amulet and mask decided instead to hold a third teen at knifepoint, in the real world, until he transferred the virtual goods to them. While obviously, holding a person at knifepoint is a crime, what was less clear at trial was whether the theft of the virtual amulet and mask constituted theft of "goods" under the traditional theft offense. RuneScape had a strict rule that goods earned within its game could not be sold. Nevertheless, it became apparent that in spite of this rule, such goods were in fact sold on eBay and the judge ruled even such virtual goods did have value and so qualified as "goods" under the statute.

This is just a short sampling of some of the more significant and, in some cases curious, changes that have occurred in cyberlaw over the past 2 decades. While the law has often had to play catch-up and in some cases took some tortuous turns, it has not stood still. New technologies and new cases testing the scope of these statutes will continue to forge and shape cyberlaw in the foreseeable future. ■

About the Author

Rick Aldrich | is the Senior Computer Network Operations Policy Analyst for the Information Assurance Technology Analysis Center. He has been awarded several grants by the Institute for National Security Studies to study the legal and policy implications of cybercrime and information warfare. He has multiple publications in this field, including a chapter on information warfare in the widely used textbook, National Security Law. He has presented at several conferences and was a primary contributor to the Cyberlaw I and II courses distributed by the DoD. He has a B.S. in Computer Science from the U.S. Air Force Academy, a J.D. from the University of California at Los Angeles, and a LL.M. in Intellectual Property Law from the University of Houston. He is also a Certified Information Systems Security Professional. He can be contacted at *iatac@dtic.com*.

References

1. The Federal Wiretap Act is codified at 18 U.S.C. 2510-2522.
2. The Stored Communications Act, which was included in ECPA, is codified at 18 U.S.C. 2701-2712.
3. The Pen Register Trap and Trace statute is codified at 18 U.S.C. 3121-3127.
4. 18 U.S.C. 2709.
5. 18 U.S.C. 2511(2)(iii)(c).
6. The computer trespasser exception is set out at 18 U.S.C. 2511(2) (i).
7. FISA was amended in the same way by the USA PATRIOT Act.
8. Wire communications were defined as communications containing the human voice that are transmitted in part by a wire or other similar method. See 18 U.S.C. § 2510(1), (18).
9. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. 107-56, Sec. 209.
10. USA PATRIOT Act, Sec. 211.
11. The CFAA is codified at 18 U.S.C. 1030.
12. National Information Infrastructure Protection Act of 1996, Pub. L. 104-294.
13. USA PATRIOT Act, Sec. 814.
14. United States v. Drew, No. CR-08-0582-GW, 6 (C.D. Cal. May 15, 2008).
15. Other items in MySpace's terms of use prohibited content that "provides any telephone numbers, street addresses, last names, URLs or email addresses."
16. 18 U.S.C. 3121-3127.
17. USA PATRIOT Act, Sec. 216.
18. 47 U.S.C. § 1002(a).
19. Docket No. 10-1259.
20. Facebook statistics, *http://www.facebook.com/press/info.php?statistics*.
21. Directive-Type Memorandum (DTM) 09-026, "Responsible and Effective Use of Internet-based Capabilities," Feb. 25, 2010, updated by Change 2, Feb. 22, 2011.
22. Washington Post, "Md. corrections department suspends Facebook policy for prospective hires," Feb. 23, 2011, at B04. *http://www.washingtonpost.com/local/md-corrections-department-suspends-facebook-policy/2011/02/22/ABoONVI_story.html*.
23. See, *e.g.,* Department of Homeland Security Management Directive 11043, Sep. 17, 2004.
24. Alice Lipowicz, "Teachable moments from NASA's social media project," Federal Computer Week, July 23, 2010. *http://fcw.com/articles/2010/07/23/nasa-learns-lessons-from-spacebook-social-media-project.aspx*.

Letter to the Editor

Q ***In general, what are the biggest challenges to mobile application security testing? I want to ensure that the applications I develop for mobile devices do not pose any significant security risks.***

A Mobile application security testing is still relatively new compared to general application testing. There are several challenges in adapting existing approaches to mobile device applications. These challenges include—

- Mobile devices usually have one user only, which is very different from systems having multiple user profiles.
- In the interest of making a mobile device easier to use, many users purposefully configure it to have weaker security settings. Many users do not know how to configure their devices to maximize security features.
- Most mobile devices do not have encryption capabilities at the network or system level; therefore, encryption must happen at a higher level.

Key organizations are investigating ways to address mobile application security and its testing more effectively. For example, the National Security Agency is looking at how the intelligence community can access Top Secret information securely from mobile devices. [1] The Open Web Application Security Project is working diligently to identify mobile device security risks and solutions to address them. It is in the process of identifying top 10 lists for mobile risks and for controls that users can implement. [2]

Overall, ensuring mobile devices are secure will remain a challenge moving forward. ■

References

1. *http://www.nextgov.com/nextgov/ng_20110325_5941.php*
2. *https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project/Roadmap*

To read more about mobile device security, read "Securing the Mobile Device…and its User" by Angela Orebaugh in this edition of the *IAnewsletter.*

▷ *continued from page 23*

SECURING THE MOBILE DEVICE…AND ITS USER

Twitter @AngelaOrebaugh and connect with her on Google+ at *http://gplus.to/angelaorebaugh.* She can be contacted at *iatac@dtic.com.*

References

1. Lieff, Laura. Mobile Spyware is Here. *http://www.glendalecherrycreek.com/t,news_template/m,news_detail?id=168.*
2. Katalov, Vladimir. ElmSoft Breaks iPhone Encryption, Offers Forensics Access to File System Dumps. *http://blog.crackpassword.com/2011/05/elcomsoft-breaks-iphone-encryption-offers-forensic-access-to-file-system-dumps/.*
3. Symantec. Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually. *http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.*
4. Hickey, Kathleen. 3 of 10 Android users now face malware attack. *http://gcn.com/articles/2011/08/03/android-hacks-rise.aspx.*
5. Brodkin, Jon. Android Trojan records phone calls. *http://www.networkworld.com/news/2011/080111-android-trojan.html.*
6. Krehel, Ondrej. Worse Than Zombies: The Mobile Botnets are Coming. *https://www.infosecisland.com/blogview/14413-Worse-Than-Zombies-The-Mobile-Botnets-Are-Coming.html.*
7. Infosecurity-magazine.com. Analyst spots major changes in Android DroidDream malware. *http://www.infosecurity-magazine.com/view/20821/analyst-spots-major-changes-in-android-droiddream-malware/.*
8. Cluley, Graham. The top 10 passcodes you should never use on your iPhone. *http://nakedsecurity.sophos.com/2011/06/14/the-top-10-passcodes-you-should-never-use-on-your-iphone/.*
9. *http://www.pcmag.com/article2/0,2817,2367247,00.asp*
10. Infosecurity.com. One in five firms have no policy regarding personal mobile device use at work. *http://www.infosecurity-us.com/view/19765/one-in-five-firms-have-no-policy-regarding-personal-mobile-device-use-at-work/.*
11. Kenyon, Henry. State Using App that Separates Personal, Work Data on iPhones, Androids. *http://gcn.com/articles/2011/06/20/west-virginia-secure-app-for-iphone-android.aspx.*
12. Government Executive. Cybersecurity and Mobility Expert Dialogues. *http://dialogues.govexec.com/govexec_archive/discussion160.html.*
13. Gillis, Tom. Doctors Love the iPad. But What's the Prescription for Table Security? *http://www.forbes.com/sites/tomgillis/2011/07/30/doctors-love-the-ipad-but-whats-the-prescription-for-tablet-security/.*
14. Marks, Josheph. Going Mobile. *http://www.nextgov.com/nextgov/ng_20110906_7177.php?oref=rss&utm_source=twitterfeed&utm_medium=twitter.*

▷ continued from page 24

suddenly appear on the employee's desktop. At the same time, this team of cyber-detectives strove to pinpoint the weaknesses that had allowed the attackers to break into the network and computing environment, and to close those holes to prevent further incursions.

To assist them, the team called in specialists in APT incident response and forensic analysis. Together, they discovered that a stealthy Trojan horse was running on the employee's computer. This Trojan turned out to be the component of a larger APT attack that began, like many APT attacks, with a "spear phishing" e-mail sent by the attackers months earlier. [2]

Spear phishing is often used by APT attackers to establish an initial presence on a targeted computer or network. In this case, the investigators traced several messages on the company's e-mail system addressed to key individuals in the company. These messages seemed perfectly legitimate—their subject lines and content were relevant to the company's business, they were written in a style consistent with e-mails generated by the company, and their From addresses originated from organizations with which the company did business. In short, there was no indication that the e-mails were not, in fact, legitimate but had been generated by an APT attacker.

APT attackers work hard to gather intelligence and build profiles of their chosen target organizations and their employees. This intelligence may be collected using standard query language (SQL) injection attacks to extract data from the target's databases. The attackers may mine personal and sensitive data they can find in online public records and across the target's aggregate Internet presence; on social media sites such as LinkedIn, Facebook, and Twitter; and elsewhere in the extensive digital paper trails that all organizations and individuals leave in the wake of their online activities. APT attackers then combine all the salient data they obtain into a comprehensive set of target-specific details they can leverage to fool employees of the targeted organization trusting the legitimacy of the attacker's carefully-crafted spear phishing e-mails.

Another typical feature of spear phishing e-mails is the inclusion of attachments. In the case of our attack, each e-mail message included an attached PDF file that several recipients opened (see Figure 1). The act of opening the file triggered the extraction of a Trojan horse program embedded in the PDF. This Trojan was designed to exploit known vulnerabilities in the version of Adobe Acrobat Reader that the attackers knew was running on the company's client computers. The vulnerabilities enabled the Trojan to infect the recipient's computer by writing itself to the Windows System32 directory, where it masqueraded as a Windows Svchost.exe system process. [3] Because the attackers had compiled the Trojan's source code only days before launching their attack, no anti-virus scanner vendor had yet had time to issue a signature to detect it.

Once executed, the Trojan established a backdoor channel from the infected computer to a Web site previously compromised by the attackers. The malware's first connection to this Web site acted as a signal to the attackers that the employee's system had been successfully compromised. The malware then requested, downloaded, installed, and executed an even more sophisticated Trojan, which established a beaconing channel to another attacker-controlled Web site. Beaconing is a reverse channel remote control technique, where all communications are initiated not by the attackers outside the target's firewall but by the malware inside the firewall. The beaconing communications by which the attacker controls the malware go undetected by the vast majority of firewalls, because most firewalls do not monitor traffic outbound from an internal trusted network, especially not Hyper Text Transfer Protocol (HTTP)/HTTP Secure (HTTPS) traffic traversing Ports 80 and 443 of the firewall.

Beaconing required the APT attackers to use a "publish and subscribe" approach—on the Web site, the attackers posted instruction sets for controlling the Trojan. The Trojan was programmed to periodically connect to the site and request new data according to a randomized schedule. This made it harder for any network monitoring tools to detect patterns or for post-incident forensic analysis to pinpoint the Trojan's requests and retrievals, because the requests seemed like legitimate Web browsing traffic initiated by the client's user; the retrievals also blended in with the company's legitimate network traffic.

On top of the Trojan's masquerading and stealth techniques, the Web servers used by the attackers were programmed to respond correctly only to requests that had HTTP headers subtly encoded to signal the servers that they had originated from the Trojan. This subtle encoding came in the form of a modification to the user-agent variable field in the header. Such a modification would be overlooked by anyone examining traffic originating from the infected computer unless that person knew specifically what to look for. Even an administrator suspicious enough go to the Web page indicated in one of the Trojan-originated HTTP headers would find only a seemingly innocuous Web page. Because that HTTP request would not include the necessary header modification the Web

server expected, the administrator's connection to the Web site would signal the attackers that their activities had been discovered, enabling them to alter their approach.

The next discovery was that having gained control of a handful of systems on the target network, the attackers had initiated a series of lateral moves into other areas of the network. The attackers did this using the internal systems under their control as launching points for attacks against other systems on the network. This enabled them to increase their network presence while eluding detection, because their expansion attacks occurred inside the network's perimeter, completely bypassing the company's perimeter security controls.

The forensic evidence revealed that the main objective of this phase of the attack was to steal as many authentication credentials as possible to access systems in the network environment. The attackers, in fact, managed to capture the credentials of most of the company's users, including all of its senior executives. The credential theft techniques the investigators suspected included the attacker's pulling Windows Security Account Manager data from system registries and Active Directory account data from the NTDIS.dit file, extracting credentials from system cache and directly from system memory, and installing keyloggers to capture passwords as they were entered by the users. The attacker were also suspected of searching networked hosts for private keys, such as those stored in X.509 PKCS#12 files, and of leveraging the processing power of a graphics processing unit to crack recovered password hashes to reveal the original passwords. The attackers may also have launched "pass-the-hash" attacks in which password hashes, rather than original clear text passwords, were submitted as authentication credentials.

The attackers used the credentials they stole to log into various computers on the network, and because these compromised credentials belonged to legitimate users, the log-ins appeared legitimate to network monitoring software and to the administrator in reviewing the system logs. The inability to distinguish attacker log-ins from legitimate user log-ins made it nearly impossible to cut off the attacker's access to network environment without issuing new credentials for all systems to all users.

APT attackers always carefully study their targets to understand how the environments operate, what technologies are used, and what weaknesses and vulnerabilities can be exploited. This enables the attackers to establish new, alternative access paths, even after their earlier paths are shut down. Indeed, APT attackers are known to go to great lengths to keep their attacks "alive." They use a variety of resiliency techniques to ensure that if one access path into a target environment is discovered and shut down, several others remain open, or new ones can be rapidly constituted. To this end, APT attackers not only seek to install malware on as many systems as possible, but to install different versions of malware across those systems. During the forensic investigation of this attack, for example, the analysts recovered four different backdoor Trojans, three of which had never been seen before. Malware diversity makes it harder to find and eradicate malware from

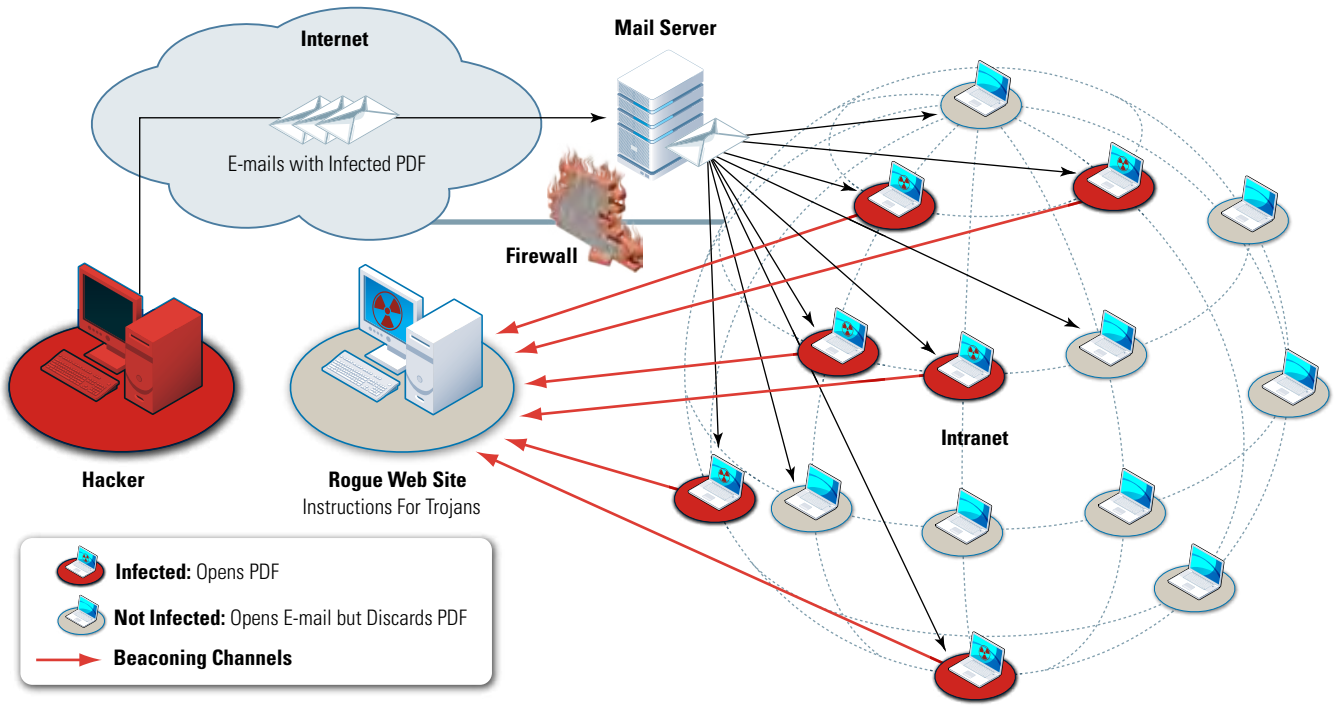


Figure 1 Spear phishing attack

infected systems. Even if one malware instance is discovered and an anti-malware signature is developed to enable anti-virus scanners to find and delete the malware from all infected systems, the other malware versions will continue to operate unimpeded until they, in turn, are discovered and eradicated.

In our incident, once the APT attackers' arsenal was entrenched in the target environment, they began locating and exfiltrating data. Typically, attackers use a variety of tools designed to collect large amounts of data and mine it for the types of information of interest to them. A rich source information is stored/archived e-mail messages, which are valuable not only for the data they contain, but for the intelligence they provide that attackers can leverage in crafting of future spear phishing campaigns. The types of information APT attackers look for most often include intellectual property (*e.g.,* industrial processes and technical approaches), competitive data (*e.g.,* pricing and strategy documents), classified information, and, in the case of APT attacks in aid of financial cybercrimes, identity and financial data (*e.g.,* social security numbers and bank account data).

Data of interest is usually extruded and then transferred to a series of "staging servers" on the Internet. In the attack under investigation, the transfer mechanism was a series of encrypted HTTPS sessions that took place well outside normal business hours, when the attackers expected the network to be dormant and less well monitored. To prepare it for transfer, the infiltrated data was compressed into RAR archive files 650KB in size (to facilitate burning them to CDROM) [4], encrypted, and password-protected. The forensic analysts were able to later decrypt the containers in which the RAR files were encapsulated, only to discover that the files inside were separately encrypted with a different algorithm and crypto key. Post-incident analysis revealed that the recovered files were only the tip of the iceberg—the attack had been going on for nearly 7 months, with evidence of multiple multi-gigabyte file transfers. It is safe to assume that every single one of the organization's important documents was now in the hands of the attackers.

In our scenario, the presence of regular high bandwidth transfers outside business hours was a key indicator of the presence of the APT. The proxy logs that captured these unexpected spikes in network utilization revealed which systems were involved in these transfers. These systems turned out to be infected with APT attack Trojans. Another indicator, once it was recognized as such, was the modified user-agent field in the attack by the Trojan's HTTP/HTTPS request headers. The response team was able to track down the Trojan processes associated with the user-agents indicated in those headers, discovering that several more systems had been infected with the Trojan.

Once those systems known or believed to contain Trojan horse infections were identified, the response team worked to determine what other actions the attackers had taken on the infected systems. From these findings, the team was able to build up a library of APT indicators they could look for when future anomalies were detected. The team also performed damage assessment and familiarized themselves with the attacker's capabilities for gaining and retaining access to the network environment, using such indicators as the credentials they discovered that the attackers had compromised to figure out which systems and accounts the attackers were operating from. Needless to say, all of the compromised credentials had to be replaced before the environment could be locked down against future attacks.

Strategy for APT Attack Response

After detecting a likely APT attack, the first step in eradicating is to determine how compromised the network environment has become. To do this—

1. Search for known indicators of compromise, such as Internet protocol addresses, domain name system names, file names, file hash values, and registry entries known to be associated with APTs. Such known indicator data can be obtained through commercial threat intelligence advisory and alert subscriptions [5], and from groups such as the Multi-State Information Sharing and Analysis Center's Cyber Threat Intelligence Coordinating Group (*http://msisac.cisecurity.org/partners/cticg.cfm*).
2. Reverse engineer any malware recovered from the compromised systems, and use the results to develop signatures for detecting the malware on other systems.
3. Employ anomaly detection systems that flag unexpected system and network activity indicative of APTs.

Once APT attackers realize they been discovered, they can turn nasty in their counterattacks. They often turn their sights to gaining access to the very computers being used by incident responders to monitor them. Even when attackers cannot gain such access, they are so good at predicting the likely actions of incident responders that they can craft their counterattacks to stay several moves ahead of the response activities. This triggers a game of "whack-a-mole," where the responders hit the attackers in one place on the network, only to have them pop up again somewhere else. Only responders engaged in a strategic approach to fighting the APT have a realistic chance of eradicating such attacks.

For this reason, the forensic analysis of the APT attack needs to be paired with a rapid vulnerability assessment that will help the responders understand the degree to which the targeted network environment can—and cannot—be defended against the attacker. These assessments need to consider not just technical vulnerabilities, but issues of procedural

security and user behavior. For example, it makes little sense to reissue credentials for all systems to every user if many users remain susceptible to new spear phishing attacks.

Unfortunately, even if efforts to eliminate all traces of an APT attack are successful, it is unlikely that APT attackers determined to target a particular organization will abandon their efforts. As long as that organization's network environment contains weaknesses and vulnerabilities, countermeasures cannot be expected to keep such APT attackers at bay for long unless those weaknesses are also dealt with.

Weaknesses and vulnerabilities commonly exploited by APTs include—

- Continued use of legacy Windows authentication protocols (LanManager, NT LAN Manager)
- Extensive caching of credentials
- Use of weak authentication techniques
- Poor password quality
- Granting end users administrative accounts/privileges
- Unmanaged computers
- Lack of formal configuration management
- Inadequate log management
- Slow or incomplete patching
- Lack of user security awareness.

Once as many vulnerabilities as possible have been remediated, it is time to kick the attackers out. Eliminating vulnerabilities will also go a long way towards protecting the environment against future incursions by APTs as well as by "common garden variety" hackers and malware.

It may seem counterintuitive, but it can be preferable to allow a long-term intrusion to continue while planning and preparing for a complete eradication of the APT, rather than implementing incremental fixes that give the attackers time to target the incremental countermeasures while locating new paths of access as previously-exploited ones are shut down. To be successful, eradication of APTs needs to be done in a coordinated way that wipes out all traces of the attacker's presence while also ensuring that all vulnerabilities that the attackers could exploit to gain a new foothold in the target environment are no longer present.

After APT eradication, the long-term integrity of the once-targeted network environment needs to start with a thorough risk assessment that acknowledges that the environment is likely to be subject to an ongoing increased threat. Establishing a "hunt team" to watch for any signs of revived APT activity can be the best way to quickly determine whether new anomalies in the environment are the result of APT-related compromises. Rapid detection of future APT indicators should trigger pinpointed responses to limit damage.

While the organization depicted in our case study was able to restore the integrity of its network environment, doing so took many months; it is a battle they are still fighting. Their employees regularly receive targeted spear phishing messages, but they now have the knowledge and ability to defend against them. When compromises do occur, they are quickly identified by the hunt team, and a well-trained, well-equipped, experienced incident response team immediately takes action to limit the damage. Outbound connections to untrusted Web sites have been blocked to frustrate APT beaconing malware. Two-factor authentication is being rolled out for all users. Most important, the organization has adopted a long-term improvement plan that directly counters the techniques most likely to be used by APT attackers.

Conclusion

What are the lessons that the engineers of information systems can learn from APTs? Consider the two adjectives that describe these threats: advanced and persistent.

APTs are advanced in their engineering and design. Their creators use several software engineering techniques that are recognized to contribute to the quality and reliability of software—

- **Intelligent Reuse of Existing Code**—Much of the malware and exploit code in APTs is reused, but what makes it so effective are the small yet powerful specific adaptations that tailor the code for its function in attacking the intended target.
- **Minimal Code Size**—The malicious agents employed in APTs tend to be single purpose and, therefore, can be very small.
- **Agent Autonomy**—APT agents, while they are controlled in terms of operating according to a series of received instructions, they have sufficient logic to operate without direct communication with an external controlling entity.
- **Diversity**—APTs employ multiple agents that perform a variety of functions, including agents who may perform the same functions but implemented differently so that the detection and elimination of one such agent will not effect the others.

In addition to advance software development techniques, APT attackers use a number of sophisticated design features to ensure the maximum effectiveness of their APTs, including—

- **Attack Adaptations based on Extensive Reconnaissance**—Most attacks on the Internet are opportunistic, targeting vulnerabilities known to exist in popular technologies or software products in hopes that those vulnerabilities will be present in the specific instances of those technologies/products used in the targeted system. APT engineers, by contrast, perform extensive reconnaissance to learn about the vulnerabilities and exploitable weaknesses of their specific targets, instead of second-guessing which

vulnerabilities might be present. APT reconnaissance techniques include direct target observation and monitoring, data mining of target owners' Web presences, and social engineering of target users. This diversity of reconnaissance techniques increases the amount of information collected and the likelihood that APT attacks engineered based on that information will be effective against the specific target.

- **Redundancy and Diversity of Attack Modes and Vectors**—Again, diversity…with redundancy. APTs combine multiple forms of malicious agents with direct exploits and attack patterns (*e.g.,* SQL injection, buffer overflow, privilege escalation) and by a hybrid (*i.e.,* malicious agents that perform direct exploits/attacks). Redundancy with diversity is achieved by implementing multiple agents with the same function, but with variations significant enough to ensure that a response that eradicates one such agent will not necessarily affect the others. Redundancy with diversity is also achieved at a higher level. Different approaches are used to achieve the same objective (*e.g.,* social engineering to fool multiple users [redundancy] into providing their plaintext authentication credentials, plus capture and cracking of multiple hashes, plus multiple pass-the-hash attacks). They all have the same objective of masquerading as and gaining privileges of an authenticated user of the system. By implementing all three, the potential for success is at least tripled.
- **Deception**—APTs are engineered to be very difficult to detect, especially while they are operating. Deception techniques include remote control through beaconing, Trojan horses that masquerade as legitimate system processes, and deceptive reconnaissance techniques (*e.g.,* spear phishing).

It is not just the APT itself that is advanced; it is the human intelligence behind it. APT attackers are highly knowledgeable about their targets, the organizations that own those targets, and cyberspace generally. Attackers are skilled at analyzing targets at a forensic level of detail. They are both creative and pragmatic in their system and software engineering approaches. They understand how to achieve software quality. Finally, they have a deep understanding of human nature, which they exploit in social engineering attacks.

The other adjective of APT is, of course, persistent. This persistence refers to the APT itself—its survivability. Persistent also refers to the humans behind APTs, who are patient and extremely determined. They do not allow failures to derail their efforts; they simply come up with new approaches to achieve their objectives. They can afford to be patient and determined because they are possessed of more-than-adequate financial and technical, as well as intellectual, resources.

Those who wish to defend against APTs would do well to study not just the attacks but the attackers, and to recognize that staying one step ahead of APTs by ramping up current approaches to information assurance and cybersecurity is not possible. What is needed is a shift from a focus on defense to a focus on survivability. Engineer systems and networks that can survive virtually all threats, then you greatly reduce the need (and resources required) to investigate, understand, protect against, and respond to each individual threat. ■

About the Authors

Ron Ritchey, Ph.D. | is Chief Scientist of the IATAC and a leading technologist specializing in IA with over 20 years experience working within the information communications technology (ICT) industry. He is widely published on network security topics including co-authoring recent books on software assurance and insider threat. He has authored courses on computer security that have been taught across the country and is a faculty member of the System Administration, Networking, and Security Institute, the Institute for Applied Network Security, and George Mason University (GMU). Dr. Ritchey holds M.B.A and B.A. degrees in computer science from GMU and a Ph.D. in IT from their School of Information Technology and Engineering.

Karen Mercedes Goertzel | is a Certified Information Systems Security Professional and leads Booz Allen's Information Security Research and Technology Intelligence Service. An expert in software assurance, ICT supply chain risk management, assured information sharing, and the insider threat to information systems, she has performed in-depth research and analysis for customers in the Department of Defense, the Intelligence Community, civil agencies, and industry in the U.S., U.K., NATO, Australia, and Canada. She was lead author/editor of Information Assurance Technology Analysis Center's State-of-the-Art Report on ICT Supply Chain Risk Management, the Insider Threat to Information Systems, and Software Assurance as well as a number of other IATAC information products and peer-reviewed journal articles and conference papers on these and other cybersecurity and information assurance topics. She can be contacted at *iatac@dtic.com.*

References

1. RAR is the compressed file format output by WinRAR archiving software.
2. *http://www.nytimes.com/2011/06/03/technology/03hack.html?pagewanted=all*
3. *http://support.microsoft.com/kb/250320*
4. Examples—these do not constitute endorsements—of such subscription services include ArcSight APT Intelligence, Fidelis Security Threat Advisory, Lofty Perch Control Systems Threat Intelligence and Situational Awareness Subscription-based Intelligence Services, McAfee Global Threat Intelligence, Verisign iDefense, Critical Intelligence ICS Cyber Situational Awareness Service.

DoDTechipedia Happenings

by Sandy Schwalb

DoDTechipedia continues to be a great place to find current science and technology stories of interest to the defense community. As mentioned in the last *IAnewsletter*, Defense Technical Information Center (DTIC) unveiled "In the News" this past spring. This feature provides current news articles from major media outlets. "In the News" provides links to material in DoDTechipedia as well as DTIC's collection of technical reports and research summaries, all of which provides "the rest of the story." A search option is also available for users to find the most up-to-date information on the topic.

"In the News" has highlighted a wide range of topics, including—

- Cybersecurity
- Feeding the troops/food safety for warfighters
- Military working dogs
- Post-traumatic stress disorder
- Tracking space debris
- Traumatic brain injury
- Unmanned systems
- Virtual training.

The topics are updated regularly and all of the material is archived on DoDTechipedia—

https://www.dodtechipedia.mil/dodwiki/display/techipedia/In+the+News.

Technology Forecast Initiative

There is a new space on DoDTechipedia that contains templates to assist customers in creating bibliographic citations. These templates include fields for specific data where customers can input a personal author, corporate authorship, the report title, a title URL, an abstract, publication date, affiliation, source, and a local file. The corporate author, title, publication date, affiliation, and source are required fields. After saving the citation, the information will appear as a page on DoDTechipedia, with links and references to files. In addition to these features, users will be able to rate the citations individually.

DoDTechipedia 101 Webinar

Do not forget that DTIC offers a monthly webinar on DoDTechipedia using Defense Connect Online (DCO). These webinars provide a general overview to get you started on DoDTechipedia, how to add content, create your personal space, and navigate the wiki. Go to *https://www.dodtechipedia.mil/dodwiki/x/UIE6Aw* for more information.

Tell us what you think!

We want DoDTechipedia to remain relevant to your mission. We ask that you take our poll, which is located on the DoDTechipedia Home Page. We will post a different question each month, such as: does your organization support the use of external collaboration tools? What is your preferred method of receiving DTIC communications? Or, did you know DTIC offers customized training through DCO? The responses help us capture a snapshot of your feedback. Creating a valuable source of information requires your input. We appreciate your participation.

Please continue to share your knowledge, assist a colleague, ask a question, post an event, start a blog, and be a part of DoDTechipedia's evolving knowledge network. To ensure that the most advanced technologies reach the warfighter tomorrow, collaborate on DoDTechipedia today.

If you have any questions or need assistance while using the wiki, contact *dodtechipedia@dtic.mil.* ■

DoDTechipedia is a project of the Under Secretary of Defense for Acquisition, Technology and Logistics; Assistant Secretary of Defense, Research & Engineering; Defense Technical Information Center; and Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer.

Social Networking and Privacy

by Dillon Friedman and Angela Orebaugh

The Internet is arguably the most significant invention of the modern age. Every dispute or argument can now be resolved simply by entering a few related keywords into a user's preferred search engine. Over the last few years, access to information has been augmented by an explosion of user-generated content, or what is more commonly referred to as "social media." People profess having expertise (real or imagined) on a topic through wiki pages, discuss important issues through their blogs, and listen to others on their favorite podcasts.

Social networking has also worked its way into the lives of millions of people. It has become nearly impossible to go online and not encounter some form of social networking. Platforms such as Facebook, Google+, LinkedIn, and Twitter all appeal to the human desire for inclusion, connectedness, knowledge, and/or validation in different ways. They also offer an innovative way to share information with a massive audience. This popularity, however, has captured the attention of many government agencies and consumer-advocacy groups as these services have opened their users up to a multitude of privacy issues.

Facebook versus Google+

When people think of social networking, they often think of Facebook. According to Facebook's Statistics page, people spend over 700 billion minutes per month on Facebook, and 50% of Facebook's 800 million active users log on to the site in a given day. [1] To join and interact on Facebook, users create profiles replete with information such as their education, employment history, music and movie taste, and date of birth. Users then create connections with friends by submitting a Friend Request, which that friend must approve, to share content between them. By default, some content, such as profile information, is shared publicly with other Facebook users. In fact, a person's profile will automatically display in search-engine results if their name is entered unless the user specifically changes their Privacy Settings.

Google+ launched in the summer of 2011, creating strong competition for Facebook in the social networking arena. Users create "Circles" and designate what data may be viewed by members of these groups. They then assign their contacts to different Circles based on their familiarity or comfort level with the person, which greatly facilitates how information is disseminated. Google+ marks Google's third attempt to enter the social networking arena after Google Wave and Google Buzz ended in early failures. Like these first two attempts, Google+ is now struggling as well. Despite reaching 25 million users in its first month and being lauded for its improved privacy protections, user posts to Google+ dropped off 42% in the fall of 2011. [2]

The original differences between Facebook and Google+ privacy platforms illustrate the biggest puzzle for individuals and social media firms alike: opt-in versus opt-out. The latter approach satisfies these firms' desire to aggregate as much information as possible, which they can then sell to marketing and analytics firms interested in improving advertising by targeting specific groups. Firms such as Facebook that rely on this as a primary revenue stream assume that all information posted is intended to be made public unless the user specifically designates otherwise (opts out). An effective opt-out system requires two things: first, that the site in question provide reasonable privacy controls for its users and, second, that the site's users understand how the controls work. While most social media sites have implemented extensive privacy controls to maintain public trust, in many cases, the controls are either too complicated or the users fail to fully understand the impact of every mouse click. Because the average user has no idea how exposed their information is and what the larger impact of that exposure could be, many governing agencies and consumer-advocacy groups support a system under which users can specifically designate how and when

their information is shared, or opt-in.

Social-Networking Regulatory Issues

The opt-in versus opt-out issue has been complicated by the differing policies in two of the largest Internet-user markets, the United States and the European Union. The European Union, whose approach has been colored by conflicts like World Wars I and II during which information was collected to persecute groups of people, has adopted a number of policies, including Directive 95/46/EC and Directive 2002/58, establishing that data collection must be opted into to properly preserve the right to privacy. As a result of this view of privacy as a human right, many companies have encountered significant pushback, most notably from Germany, for perceived privacy issues. For example, over the last 2 years German courts have launched investigations into various functions on Facebook, such as the *Like* button and facial-recognition technology. [4, 5] Although Google+'s level of success in Europe is unknown at this time, its opt-in structure suggests that it will garner less scrutiny from European governments.

The United States, by contrast, takes what is referred to as a "sectoral" approach to data-protection legislation. Privacy legislation in the United States is adopted generally when certain issues arise or developments in certain industries require it, though the individual's right to privacy has been ruled as implicit in the First Amendment. Generally speaking, the Federal Trade Commission is responsible for enforcing privacy statutes, but depending on the industry of the firm in question, enforcement can also fall to the Department of Transportation, the Department of Health and Human Services, the Federal Reserve, or the Comptroller of the Currency.

To date, the social networking industry has not been the subject of any one discrete piece of legislation, though several have been deemed relevant by policymakers. Many of the founders of today's popular social networking sites had barely been born when the Electronic Communications Privacy Act of 1986 (ECPA) was passed, long before the Internet became as ubiquitous as it is today. Because ECPA's privacy provisions have not been updated since 1986, the legislation allows law enforcement and/or the government to access any information stored on a third-party server with nothing more than a subpoena. By contrast, under the federal Wiretap Act, a law-enforcement agency wanting to tap a phone must have a warrant signed by a judge, with few exceptions. Frequent lobbying attempts to strengthen the requirements for accessing information stored on a third-party server have thus far proven unsuccessful. [6]

Another piece of legislation related to social networking is the Children's Online Privacy Protection Act of 1998 (COPPA), which delineates how a commercial Web site directed at children under 13 years of age may collect and use data. COPPA also limits the information an operator can provide to advertisers without parental consent. Given the indiscriminate data-collection practices of many social networking sites, several, including Facebook, MySpace, and Twitter, do not allow children under the age of 13 to join their sites, and Google+ is currently only available to users 18 and over. It bears mentioning that Facebook was recently called to testify on Capitol Hill regarding how it protects children online.

Beyond legislation, social networking sites have proven responsive to the free market. For example, in August 2011, LinkedIn tried to implement "social ads," a new form of advertising that attached users' names and pictures to product endorsements. The blog post notifying LinkedIn users of this new development generated no substantial response, but when users actually saw the ads, the outcry was swift. Within a week, Ryan Roslansky, LinkedIn's Director of Product Management, published a blog post indicating that the company would no longer make use of users' names and

photos in ads. Instead, social ads now only inform users when a person in their network recommends a product or follows a company, however, LinkedIn users are still automatically opted-in to this social advertising. Users may opt out by going to *Settings* > *Account* > *Manage Social Advertising* and unchecking the *Linked In may use my name, photo in social advertising* check box.

General Social-Networking Privacy Recommendations

When using social networking services, it is important to understand the various privacy settings, select the most secure options, and periodically check for changes to options and settings. The following general privacy guidelines apply to social networking, regardless of platform—

- **Use your brain**—Although it sounds like common sense, the most important privacy feature is to think before you post. Status updates, photos, and comments can unintentionally reveal personal information. Do not include information that could give away personal or sensitive information about yourself or others. For example, some users do not reveal the names of their children, pets, or address online. It is also best to avoid the often-circulated surveys and questionnaires that request personal information.
- **Private may not be private**—Treat private messaging the same as public, as you never know when you are mistakenly cross-posting, or when messages could be leaked to the public. Also, many companies still retain records of private messages, even if they are not reviewing the content.
- **Applications do more than you think**—Consider the applications that you install and the information to which they request access, and remove applications that you are no longer using.
- **People are watching**—Be mindful of geo-location services such as Foursquare and built in check-in services on Facebook and other platforms. These services reveal your exact location, let criminals know you are not home, and could also reveal other information about your personal preferences.

Facebook Privacy Recommendations

Competition with Google+ has forced Facebook to improve how it addresses users' privacy concerns. Facebook created a Director of Privacy position and appointed Erin Egan, a privacy and data-security lawyer formerly with Covington and Burling. Starting in August 2011, Facebook began allowing users more direct control over who can access uploaded content. Facebook's List feature, with similar advantages as Google+ Circles, and "inline" privacy settings for posts, pictures, and status updates, have greatly simplified how Facebook users protect their information. Facebook users should be aware of the following privacy settings and best practices—

- **Friend Lists**—Facebook allows you to create custom lists of people to share content with and to use in sharing different aspects of your profile. You may configure these lists to be as simple as Friends, Family, and Professional, or you may get more detailed with Book Club, Work Friends, High School Friends, *etc*. Use the various lists to enable the most granular privacy settings.
- **Tagging**—By default, your friends can tag you in posts and photos, which will automatically show up on your profile. For privacy, enable Profile Review in the Tags section of the Privacy Settings to manually review and approve posts (including photos and videos) that you are tagged in before they appear on your profile. Remember that the posts and photos tagged with your name will still show up on the person's wall who posted it, but not your wall until you approve it. If you remove the tag you can also send a message to the user who tagged you, requesting that they remove the post or photo, and you can also block that person entirely. Also note that any post or photo in which you tag someone is viewable by the person you tagged. Customize the Tag Review feature in Privacy settings to approve or reject tags that friends post.
- **Search Visibility**—By default, some of your Facebook profile information will show up in Web searches. You can remove your profile from being displayed in Web search results by disabling Public search through *Privacy Settings* > *Apps, Games, and Websites* > *Public Search*.
- **Friend Visibility**—Your Friend List is visible to anyone by default unless you disable this feature. To make changes, choose *Edit Profile* > *Friends and Family*. You will see the drop-down option next to Friends that allows you to configure who can see your Friend List. This can be set to public, only you, friends, or any other custom list you have created.
- **Application Access**—Some applications have optional access that can be revoked. For example, many popular applications have a control that allows access to your data at any time, even when you are not using the application. This control option can be removed. Also, when reviewing applications, there are privacy settings for each application to limit who can see posts and activity from that application. Finally, remove applications you are no longer using.
- **Inline Privacy Controls for Content**—Take advantage of the individual privacy settings. You can choose specific lists for sharing posts, photo albums, individual

photos, and various elements of your profile. Each of these pieces of content has a drop-down box next to it for inline privacy controls. You can also use the *View As…* button on your profile to see how your profile is visible to others.

Google+ Privacy Recommendations

Google+'s inline controls and Circles give it a competitive advantage in social-networking privacy. For even more information in Google+ privacy, you can access the Privacy Center from the Profile and Privacy section of your Account Settings page. Privacy Center centralizes privacy features for many of Google's products and services. One significant difference with Google+ is that anyone using the service can add you to his or her circles; there is no request process as with Facebook. But just because someone has added you does not mean they can see any of your information if you are using the inline controls appropriately, although they, and everyone else, will see anything you designate as Public. Google+ users should be aware of the following privacy settings and best practices—

- **Circles**—Google+ privacy is built on Circles—groups of people you share content with. The names of your Circles and those you add to them are visible only to you. Build Circles such as friends, family, and professional colleagues to enable the granular privacy capabilities.
- **Profile Privacy**—When editing your profile, each element has a drop-down menu associated with it to allow you to share that element with specific Circles. Your Full Name is the only required element in the profile, and is visible to anyone on the Web. You can customize your privacy for each element to reflect what you are comfortable sharing. You can also use the *View Profile As…* check box on your profile to see how your profile is visible to others.
- **Profile Discovery**—By default, your name and any other fields you make public in your profile are searchable on the Web. If you are concerned about your profile showing up in search engines, you can disable this by editing the Profile Discovery in your Profile and clearing the Help others discover my profile in search results check box. This will block search engines from indexing your profile.
- **Circle Visibility**—By default, anyone on the Web can see whom you have added to your Circles (but not which specific Circle) and who has added you to their Circles. To change this, on the left side of your profile, click the *Change who is visible here* link. You can choose to hide both of these elements from everyone, or to make them available only to certain Circles.
- **Geo Location**—By default, Google+ shows geo-location tagging for photos. You can limit the use of geo-tagging by disabling photo geo-tagging in the Google+ section of your Account Settings page. Clear the *Show photo geo-location information in newly uploaded albums and photos* check box.
- **Tagging**—You can disable or pre-approve individuals or Circles to tag you in photos and link to your profile. You can also limit the use of photo tagging by selecting or removing those individuals or Circles that you automatically approve to link to your profile by editing the Photos permissions in the Google+ section of your Account Settings page, or by selecting the Photos tab while editing your profile.
- **Post Privacy**—You can use the inline privacy settings to select individuals and Circles with which to share any post you write. For each new post, Google+ remembers the individuals or Circles you shared with last, so it is wise to check this setting each time you post. You can also disable comments and lock the post from sharing before submitting. Note that your comments on other people's posts are shared with the same privacy as that post; therefore, if you…if you comment on a publicly shared post, your comment will be public and searchable on the Web. Check to see if the post privacy setting is Limited or Public to gauge who will be able to read it.
- **Understand +1's**—The Google +1 feature allows you to share information publicly, but is also recorded for Google and its partners. This information may also appear to others as an annotation with your profile name and photo in Google services and on the Web. You can view the list of items that you have designated as +1 on the +1 tab of your profile. You can also remove items from the list. While editing your profile, clicking the +1 tab will allow you the option to hide the tab from others viewing your profile.

The long-term significance of online social networking remains to be seen as technological advancements are continuously revolutionizing the way we interact. We have only just begun to understand how these new means of collaboration and communication will shape our daily lives or even the world. Events like the recent uprisings in Iran and Egypt demonstrate how social networking platforms are being used to challenge authoritarianism, while the London riots in the summer of 2011 highlight the dangers of an idle population empowered by Twitter and Blackberry Messenger. The next generation, which will have grown up with the likes of Facebook and Google+, will face the task of determining how these technologies evolve and affect the right to privacy.

▷ ▷ *continued on page 50*

Software Security Tactics

by Jungwoo Ryoo, Phillip Laplante, and Rick Kazman

The scope of security control mechanisms varies widely depending on their focus. One of the most comprehensive security control approaches is the Common Vulnerability Scoring System (CVSS) by the CVSS-Special Interest Group. CVSS is an open and standardized vulnerability scoring system for rating information systems security vulnerabilities in general. [1] Software security is simply one of the concerns out of many addressed by CVSS. Among the 14 CVSS metrics, exploitability might be the only metric directly related to software security. Other metrics assess broader security controls, such as access complexity, collateral damage potential, authentication, *etc.*

Since the coverage of software security vulnerability is relatively weak, efforts have been made to develop a framework to more directly examine software security weaknesses. For example, the SysAdmin, Audit, Network, Security (SANS) Institute in collaboration with the MITRE Corporation has identified the top 25 most dangerous software errors. [2] Although concentrating solely on software vulnerabilities, the SANS list puts almost all of its emphasis on programming errors. For example, one of the items listed under the Insecure Interaction between Components is improper neutralization of special elements used in a Standard Query Language (SQL) Command (SQL Injection). Considering that a typical software development life cycle consists of multiple phases and programming is only one of these phases, it may be prudent to also look into the other phases in an effort to reduce the number of vulnerabilities found in software products.

Software is transformed through multiple levels of representation during its lifetime, which implies that software security is a multi-level concept.

The top 25 software errors list heavily relies on the Common Weakness Enumeration (CWE) system. [3] In fact, the SANS Institute simply categorizes and prioritizes the existing CWE items. This trend of programming-centric software vulnerability mitigation culminated in a recent introduction of the Common Weakness Scoring System (CWSS). The MITRE Corporation maintains CWSS for the Department of Homeland Security (DHS). The aim of CWSS is to raise awareness and better educate programmers to avoid common programming errors that usually lead to software security vulnerabilities exploited by hackers. In addition, programmers will be more closely scrutinized and evaluated regarding their effectiveness in adopting secure coding practices.

These new developments in the software security community are a step in the right direction since the focal point of the mitigation effort is now shifting from detecting programming errors after they have been committed to prevention. Until recently, one of the most dominant software security intervention methods was the static analyses of completed programs. A good example of this is a DHS-sponsored project to scan popular open source software for vulnerabilities. [4]

We believe that the current emphasis on coding errors must evolve into an even broader set of interventions that encompass all aspects of software security, including requirements elicitation and software design. Although the coding error detection techniques may effectively identify and remove flaws in the source code, they cannot do the same for the improper software architectures or lower-level designs that actually originated the security vulnerabilities.

Software is transformed through multiple levels of representation during its lifetime, which implies that software security is a multi-level concept. As

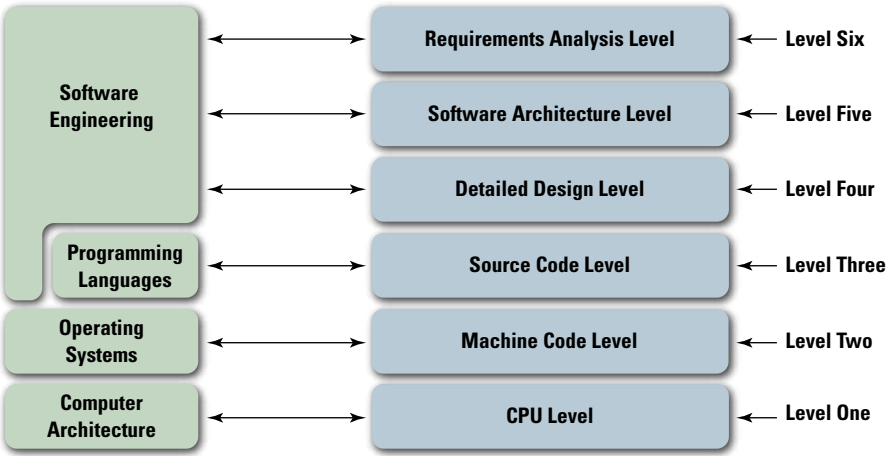


Figure 1 Different levels for software security

shown in Figure 1, at the bottom level (referred to as the central processing unit [CPU] level in this article), in its final delivered form, software is executed as sequences of instructions on one or more CPUs. Before running on processors, the software exists as machine code in different layers of the storage hierarchy of a computer. Programmers must, of course, write the source code prior to compilation. Detailed design precedes the source code production process after a solid software architecture is established. The beginning level is a phase dedicated to analyzing user requirements (Level Six).

Researchers in various disciplines (shown as rounded squares in the left-hand side of Figure 1) are making efforts to address security at each of these levels discussed so far. For each security threat, several countermeasures could be deployed at multiple levels with different sets of advantages and disadvantages; although, deployment at one level is sometimes much more effective than other alternatives.

We are particularly interested in secure software design, especially at the software architecture level. Our contention is that security must be considered from the beginning and then built into a program, rather than adding security features as afterthoughts. [5,6] An analogy in building architectures could be the different architectural styles used for bomb shelters and residential buildings. Adding security bars and cameras cannot turn an apartment building into a proper bomb shelter.

Secure Software Design

While not as highly advertised as secure coding practices and static code analyses, there are also a substantial number of communities attempting to archive secure software design practices. The members of these communities argue that it is possible to identify and capture recurring security design solutions and reuse them. They refer to these security design solutions as security patterns. [7]

There are two broad types of security patterns: one aimed at solving purely local design problems and the other tackling global design challenges affecting the entire software architecture. The former pattern type is referred to as a design pattern while the latter is referred to as an architectural pattern. Design patterns deal with more immediate, problem-specific tasks such as how to avoid buffer overflows. The architectural patterns, however, cope with global concerns such as how to minimize the number of entry points into a software component. The ultimate goal of the patterns communities is to provide a comprehensive catalogue of both architectural and design patterns so that software practitioners can pick and choose the most appropriate design solutions for their problem at hand without having to develop their own solutions from scratch every time. This speeds up the design process and allows

a software designer to build on a proven solution.

One of the shortcomings of the patterns we use today is that they are not highly malleable. When software designers begin to reason about potential design solutions during the architectural phase, they do not have sufficient information and insight yet to make the mature design decisions that are usually manifested in the architectural and design patterns. We contend that software architects require more primitive design building blocks that they can use to explore design options before fully committing themselves to a final solution. Additionally, it would be ideal if the architects could compose these design building blocks into custom design patterns and simply use existing design patterns as their reference models.

Security Tactics

Due to the need for more fine-grained control over architectural decisions, a new set of design primitives, called a tactic, have been catalogued. [8, 9, 10] A Tactic is an atomic design primitive intended for a software architect to reason about architectural design solutions that directly affect a single software quality attribute such as security, without considering other quality attributes such as performance, modifiability, usability, *etc.*

For example, a design solution, such as minimizing the number of entry points (*i.e.,* Limit Exposure), is a tactic because the tactic only affects the security quality attribute. An architect does not have to be concerned about how it will affect the other quality attributes of an architecture, such as performance. The Limit Exposure tactic cannot be further decomposed into more fundamental and primitive design solutions either.

Layers are a well-known architectural pattern. In networking and telecommunications, the Layers architectural pattern plays a major role in organizing various standards into different layers. Standards such as Hyper Text Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP) belong to the Application Layer. The developers of these Application Layer standards do not have to know anything about how messages are delivered from one host to the other since the layers below (*i.e.,* Transport, Internet, Data Link, and Physical) handle the delivery of the messages. In this way, the Application Layer standards developers can simply focus on how the two hosts interact with each other to do something meaningful for end users (*e.g.,* interactions between a Web browser and a Web server).

Layers are an architectural pattern and, as such, affect multiple quality attributes. For example, changes in one layer do not affect the other layers and are kept local (modifiability). A layer developed for one architecture can be reused for another (reusability).

Building the Limit Exposure tactic into an existing pattern is also possible. An example for this is the use of encryption at different layers of the layered network architecture. Encryption can be used at either the Transport layer or the Internet layer to limit exposure and results in a more secure version of the layered architecture. The benefits of tactics are now more obvious from our discussion of the relationship between tactics and architectural patterns. Tactics are used to refine architectural patterns. This is useful because patterns are intentionally underspecified to leave room for customization and enhancement based on the needs of a particular problem at hand. It is also possible to compose an entirely new architectural pattern, using tactics if none of the existing architectural patterns are able to solve a given problem.

Because the nature and usage of tactics and architectural patterns are significantly different, it is critical to keep tactics clearly separated from patterns to avoid misuse and confusion.

Security tactics are still in the early stages of discovery, at least as compared to security patterns.

The reality is, however, far from this ideal situation.

The known set of security tactics can be described in a single hierarchy based on the following three categories: (1) resisting attacks, (2) detecting attacks, and (3) recovering from an attack. [8] Individual tactics are then categorized as shown in Figure 2.

Consider some of the tactics in the first category. There are a number of well-known means of resisting an attack—

- **Maintain Data Confidentiality**—Data should be protected from unauthorized access. Confidentiality is usually achieved by applying some form of encryption to data and communication. Encryption provides extra protection to persistently maintain data beyond that available from authorization. Communication links, on the other hand, typically do not have authorization controls. Encryption is the only protection for passing data over publicly accessible communication links. The link can be implemented by a virtual private network or by a Secure Sockets Layer for a Web-based link. Encryption can be symmetric (both parties use the same key) or asymmetric (public and private keys).
- **Maintain Integrity**—This tactic encodes redundant information in data such as checksums or hash results, which can be encrypted either along with or independently

from the original data. This allows the recipient or reader to verify that the data has not been modified either in transit or at rest.

- **Limit Exposure**—Attacks typically depend on exploiting weaknesses to gain access to data and services on a host. The Limit Exposure tactic minimizes the attack surface of a system. [11] This tactic focuses on reducing the probability and minimizing the effects of damage caused by a hostile action. It is a passive defense since it does not proactively prevent attackers from doing harm. The Limit Exposure tactic is typically realized by having a small number of access points for resources, data, or services.
- **Limit Access**—This is a category of widely used security tactics that restrict access to resources, data, and services to only authorized actors. For example, a demilitarized zone is used when an organization wants to let external users access certain services and not access other services. It sits between the Internet and a firewall in front of the internal intranet. The firewall is a single point of access to the intranet (Limit Exposure). It also restricts access using a variety of techniques to authorized users (Limit Access).

The use of a tactic does not eliminate trade-offs—the effect of the tactic on the quality attributes other than the one it directly targets; however, a tactic allows an architect to focus on identifying the right solution to a given design task by providing a systematic catalogue of available design options without having to worry about the trade-offs yet. Unlike tactics, patterns do not provide this detailed level of control over design outcomes.

Once the initial decisions are made on which tactics to use, a pattern might then be selected, which incorporates two or more of the chosen tactics. Using this new design fragment, a software architect can now reason about the effects of the selected tactics on each other, seeking balanced solutions and trade-offs grounded on the reality of the requirements of the software being developed.

It is important to understand the potential combinations of tactics and patterns in a design process. Sometimes an architect chooses a pattern and then augments it using tactics. Other times, the architect might choose a tactic and then choose a pattern that encompasses it. The relationship between tactic and pattern is akin to that of an atom and molecule (*i.e.*, one encompasses the other) rather than temporal ordering.

Currently, most practitioners skip the tactics stage and jump directly into the patterns stage, which makes the design process more challenging and often overwhelming. The contribution of tactics is to provide a divide-and-conquer approach that partitions the early design phase into the tactics and patterns stages, providing more design options and control over quality attribute outcomes to the architect.

Tactics are differentiated from patterns since they are more primitive building blocks that are eventually woven together into a pattern. As of this writing, the boundaries between tactics and patterns are not clearly distinguished in the research and practice literature. In fact, many tactics seem to be misidentified as patterns due to the lack of awareness of the concept of a tactic. One of our research goals is to identify the tactics misclassified as patterns and to reclassify them as tactics.

The main criteria used to discern tactics from patterns are as follows—

- **Atomic Design Operation**—Can it be decomposed into design choices that directly affect individual quality attributes? If so, it is a pattern; otherwise, it is a tactic.
- **Problem-specificity**—Is it application domain-specific? If so, it is a pattern; otherwise, it is a tactic.
- **Force Limitation**—Does it affect more than one quality attribute? If so, it is a pattern; otherwise, it is a tactic.
- **Tradeoffs between Forces**—Is there a need to worry about multiple, conflicting quality attribute requirements? If so, it is a pattern; otherwise, it is a tactic.
- **Completeness**—Is it underspecified or incomplete? If so, it is a pattern; otherwise, it is a tactic.

Security tactics are still in the early stages of discovery, at least as compared to security patterns. There is no widely accepted mechanism for discovering these tactics, nor a conventional way to categorize security tactics and to eventually gain consensus in the

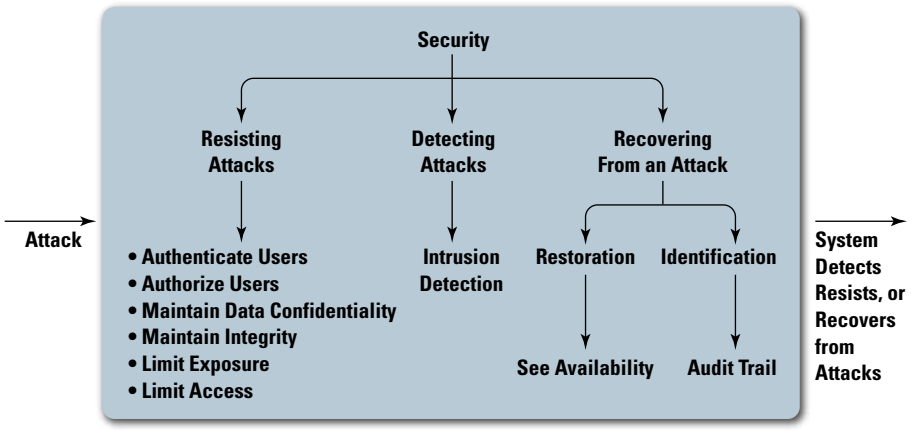


Figure 2 A hierarchy of security tactics

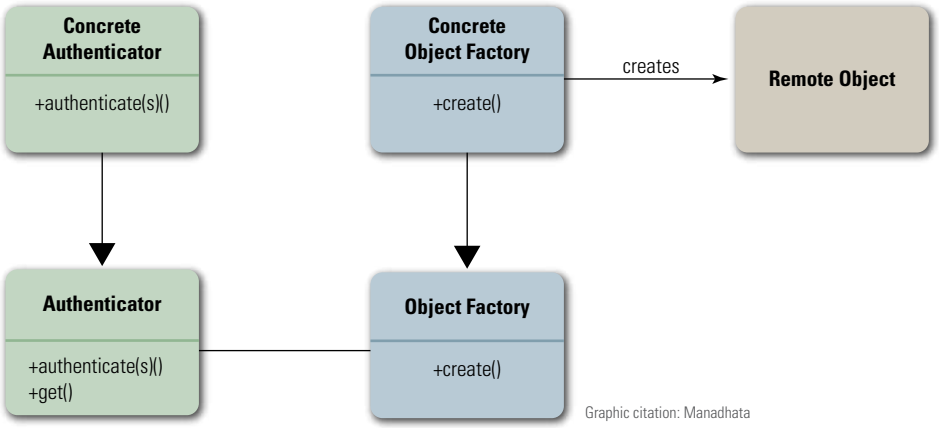


Figure 3 A UML diagram for the authenticator pattern

research community in this area, but we are working on several approaches. [10]

Examples *(These sections are adapted from [10])*

Consider the two relatively straightforward scenarios given below. These scenarios demonstrate how the criteria described in the previous section can be used to either confirm the validity of a pattern or reclassify the existing security patterns into tactics.

In the first scenario, the authenticator pattern is used to demonstrate how a candidate pattern is categorically denied reclassification. [12] This rejection process also shows how some tactics can be salvaged as byproducts in the process.

According to Brown *et al.,* "The authenticator pattern performs authentication of a requesting process before deciding access to distributed objects." [12] This description already gives a strong impression that the pattern is strongly tied to a specific problem domain. Phrases such as "requesting process" and "distributed objects" strongly suggest domain specificity. It is obvious that the authenticator pattern does not meet the problem specificity condition.

Figure 3 shows that the authenticator pattern is relying on another pattern (*i.e.,* factory method). The factory method pattern can then be decomposed into the information hiding tactic (through the use of an interface) and the intermediary tactic, both of which promote the modifiability quality attribute of the software. Based on these facts, we can conclude that the authenticator pattern violates the atomicity, force limitation, completeness conditions. The pattern also violates the tradeoffs between forces condition since the contention between security and modifiability is present.

Although the authenticator pattern itself is disqualified as a tactic, one might still be able to recognize a tactic behind the pattern, which is authenticate users. Nonetheless, the recovered tactic is already a known one in this case.

The second scenario involves a pattern that is clearly misidentified and should be reclassified as a tactic. The pattern is referred to as compartmentalization. [13, 14] The pattern is described as "put each part in a separate security domain. Even when the security of one part is compromised, the other parts remain secure." Unlike the authenticator pattern discussed earlier, this description does not have anything indicating problem specificity. It is also atomic and satisfies the force limitation (addressing only the security quality attribute), completeness, and tradeoffs between forces conditions; therefore, the compartmentalization pattern should be reclassified as a tactic. In the tactics hierarchy (Figure 2), the new tactic should be placed under the Limit Access tactic.

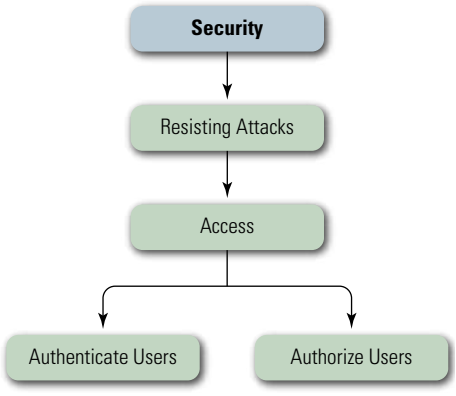


Figure 4 An example of restructuring the security tactics hierarchy

Future Research Directions

The security tactics hierarchy depicted in Figure 2 appears to be relatively flat, suggesting ample room for many more intermediate nodes in the graph. A richer hierarchy will naturally develop as newly discovered tactics fill the gap. Some of the existing tactic categories can also be extended to include subcategories by borrowing the criteria already used for classifying security patterns. For example, the Maintain Data Confidentiality and Maintain Integrity tactics can become branches of their own right and be further refined with their offspring (*i.e.,* additional security patterns that could well be reclassified as tactics, which are currently grouped into security domain concepts like confidentiality and integrity respectively). In addition, based on the commonly accepted categorizations of security countermeasures in the security community, the Limit Access tactic and the Authenticate Users and Authorize Users categories can be rearranged as shown in Figure 4.

Our ultimate goal is to be able to add new concrete tactics under each of the leaf nodes in the newly enhanced graph, such as the Authenticate Users and Authorize Users categories, and to add new mid-level nodes. This will provide a richer and hopefully more complete set of building blocks for

security patterns. [18] To this end, we are conducting a survey of software security practitioners to expand the knowledge of software security tactics.

The Survey

Our research is currently at the data collection stage. We recognize that reaching a consensus on the precise definitions of tactics and their relationships with patterns is a critical part of verifying the validity of our research accomplishments so far. After all, a large part of patterns identified until now have gone through this community process. For this reason, we are conducting a survey in which we provide the participants with some candidate tactics currently labeled as patterns in the research community, along with their definitions. The participants are then asked to decide which of these are design primitives (atoms) and hence should be reclassified as tactics and which should remain as patterns. Each of the candidate tactics is described by a natural language definition extracted from the research literature. We also ask the participants whether they agree with our definitions of what tactics and patterns are.

The survey can be found at *http://tinyurl.com/4xr9e5w,* and we encourage interested readers to participate. ■

About the Authors

Jungwoo Ryoo, Ph.D. | is an associate professor of Information Sciences and Technology at the Pennsylvania State University-Altoona. His research interests include information assurance and security, software engineering, and computer networking. He is the author of numerous academic articles and conducts extensive research in software security, network/cybersecurity, security management (particularly in the government sector), software architectures, architecture description languages, object-oriented software development, formal methods, and requirements engineering. Many of Dr. Ryoo's research projects have been funded by both state and federal government agencies. He also has substantial industry experience in architecting and implementing secure, high-performance software for large-scale network management systems. He received his Ph.D. in Computer Science from the University of Kansas in 2005. He can be contacted at *jryoo@psu.edu.*

Phil Laplante, Ph.D. | is a professor of software engineering at Penn State's Great Valley Graduate Professional Center. He spent several years as a software engineer and project manager working on avionics (including the space shuttle), computer-aided design, and software test systems. He has authored and edited 26 books and has published more than 150 papers. His interests are in software and systems engineering, project management, and software testing and security. He can be contacted at *plaplante@gv.psu.edu.*

Rick Kazman | is a professor at the University of Hawaii and a visiting scientist (and former senior member of the technical staff) at the Software Engineering Institute of Carnegie Mellon University. His primary research interests are software architecture, design and analysis tools, software visualization, and software engineering economics. He also has interests in human-computer interaction and information retrieval. Mr. Kazman has created several highly influential methods and tools for architecture analysis, including the Software Architecture Analysis Method, the Architecture Tradeoff Analysis Method, and the Dali architecture reverse engineering tool. He is the author of over 100 papers and co-author of several books, including Software Architecture in Practice and Evaluating Software Architectures: Methods and Case Studies. He can be contacted at *kazman@hawaii.edu.*

References

1. Forum of Incident Response and Security Teams (FIRST), "Common Vulnerability Scoring Systems (CVSS-SIG)", *http://www.first.org/cvss,* retrieved on 9/17/11.
2. The SANS Institute, "CWE/SANS TOP 25 Most Dangerous Software Errors", *http://www.sans.org/top25-software-errors,* retrieved on 9/17/11.
3. The MITRE Corporation, "Common Weakness Enumeration," September 2011, *http://cwe.mitre.org,* retrieved on 9/17/11.
4. PR Newswire, "Coverity Selected in Department of Homeland Security Software Initiative," *http://www.prnewswire.com/news-releases/coverity-selected-in-department-of-homeland-security-software-initiative-53407882.html,* retrieved on 9/17/11.
5. Department of Homeland Security, "Build Security In", *https://buildsecurityin.us-cert.gov/bsi/home.html,* retrieved on 9/17/11.
6. McGraw, Gary, "Software Security: Building Security In", Addison-Wesley Professional, February 2006.
7. SecurityPatterns.ORG, "Welcome to SecurityPatterns.org", *http://www.securitypatterns.org,* retrieved on 9/17/11.
8. Bass, Len, Clements, Paul, & Kazman, Rick, Software Architecture in Practice, Addison-Wesley Professional, 2nd edition, April 2003.
9. Ryoo, Jungwoo, Laplante, Phillip, & Kazman, Rick, "In Search of Architectural Patterns for Software Security", IEEE Computer, vol. 42, no. 6, pages 98-100, June 2009.
10. Ryoo, Jungwoo, Laplante, Phillip, & Kazman, Rick, "A Methodology for Mining Security Tactics from Security Patterns", The 43rd Hawaii International Conference on System Sciences, Koloa, Kauai, Hawaii, USA, The IEEE Computer Society Press, January 2010.
11. Manadhata, Pratyusa K. & Wing, Jeannette M., "An Attack Surface Metric," USENIX Security Workshop on Security Metrics (MetriCon), Vancouver, BC, August 2006.
12. Brown, F, DiVietri, F, Villegas, G, & Fernandez, E, "The Authenticator Pattern," Pattern Languages of Programs 1999, Monticello, IL, 1999.
13. Hafiz, M, Johnson, R. E., & Afandi, R, "The Security Architecture of qmail." The 11th Conference on Pattern Languages of Programs, 2004.
14. Halkidis, S, Chatzigeorgiou, A, & Stephanides, G., "A Qualitative Analysis of Software Security Patterns," Computers and Security, vol. 25, pages 379-392, 2006.

USSTRATCOM Cyber and Space Symposium

The United States Strategic Command (USSTRATCOM) Cyber and Space Symposium took place November 15-17, 2011, in Omaha, NE. The conference provided an opportunity for leaders to discuss cyber innovations and ways for industry and government organizations to more effectively collaborate. It featured speakers from across the Department of Defense, U.S. government, industry, academia, and allied governments.

Some of the featured speakers included General C. Robert Kehler, USSTRATCOM Commander; General Keith Alexander, U.S. Cyber Command Commander; Admiral James Winnefeld, Jr., Vice Chairman of the Joint Chiefs of Staff; and The Honorable Howard Schmidt, White House Cybersecurity Coordinator.

This conference featured 16 different panel discussions that focused on a variety of critical information assurance (IA) and cybersecurity (CS) topics. These topics included managing risk across networks; international cyber issues and how to collaborate across borders; space and cyber solutions; and industry innovations in both cyber and space. The symposium also held academic sessions for high school students to interact with IA/CS professionals, learn more about the challenges that the field will face in the future, and gain insight into the opportunities they will have to contribute to the advancement of IA/CS in the future. [1] ■

References

1. *http://www.afcea.org/events/stratcom/11/introduction.asp*

▷ *continued from page 43*

SOCIAL NETWORKING AND PRIVACY

About the Authors

Dillon Friedman | currently works in privacy and information management and is focused on privacy and security issues concerning mobile and wireless technology as well as social media. Mr. Friedman holds a B.A. from the University of San Diego. He can be contacted at *friedman_dillon@bah.com.*

Angela Orebaugh | is a technologist, researcher, and cybersecurity executive, who is passionate about helping clients embrace tomorrow's technology today. Ms. Orebaugh was recently selected as Booz Allen Hamilton's first and currently only Cyber Fellow, a distinction reserved for an elite group of the firm's most noted authorities. She evangelizes social media and mobile technologies by highlighting the powerful ways in which these technologies are changing business, communications, and information sharing. Ms. Orebaugh is also the Information Assurance Technology Analysis Center Director of Research and Academic Integration. She is an international author and invited speaker for technology and security events. Follow her on Twitter @AngelaOrebaugh and connect with her on Google+ at http://gplus.to/angelaorebaugh. She can be contacted at *iatac@dtic.com.*

References

1. *https://www.facebook.com/press/info.php?statistics* [2]*http://www.boston.com/business/technology/articles/2011/09/15/will_google_strike_out_of_the_social_netwo* rking_market/
2. *http://www.bbc.co.uk/news/technology-14859813*
3. *http://www.pcmag.com/article2/0,2817,2390440,00.asp*
4. *http://notwithoutawarrant.com/*

FREE Products Order Form

Instructions: All IATAC LIMITED DISTRIBUTION reports are distributed through DTIC. If you are not a registered DTIC user, you must do so prior to ordering any IATAC products (unless you are DoD or Government personnel). To register online: *http://www.dtic.mil/dtic/registration.* The *IAnewsletter* is UNLIMITED DISTRIBUTION and may be requested directly from IATAC.

Name _____ DTIC User Code _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

Please check one: ☐ USA ☐ USMC ☐ USN ☐ USAF ☐ DoD ☐ Industry ☐ Academia ☐ Government ☐ Other

Please list the Government program(s)/project(s) that the product(s) will be used to support: _____

_____

LIMITED DISTRIBUTION

IA Tools Reports ☐ **Firewalls** ☐ **Intrusion Detection** ☐ **Vulnerability Analysis** ☐ **Malware**

Critical Review and Technology Assessment (CR/TA) Reports
- ☐ Biometrics (soft copy only)
- ☐ Configuration Management (soft copy only)
- ☐ Defense in Depth (soft copy only)
- ☐ Data Mining (soft copy only)
- ☐ IA Metrics (soft copy only)
- ☐ Network Centric Warfare (soft copy only)
- ☐ Wireless Wide Area Network (WWAN) Security
- ☐ Exploring Biotechnology (soft copy only)
- ☐ Computer Forensics (soft copy only. DTIC user code MUST be supplied before this report is shipped)

State-of-the-Art Reports (SOARs)
- ☐ Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain (DTIC user code must be supplied before this report is shipped)
- ☐ Measuring Cybersecurity and Information Assurance
- ☐ The Insider Threat to Information Systems (DTIC user code must be supplied before this report will be shipped)
- ☐ A Comprehensive Review of Common Needs and Capability Gaps
- ☐ Software Security Assurance
- ☐ IO/IA Visualization Technologies (soft copy only)
- ☐ Modeling & Simulation for IA (soft copy only)
- ☐ Malicious Code (soft copy only)
- ☐ Data Embedding for IA (soft copy only)

UNLIMITED DISTRIBUTION

IAnewsletter hardcopies are available to order. Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

Volumes 12	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 13	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 14	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 15	☐ No. 1			

SOFTCOPY DISTRIBUTION

The following are available by e-mail distribution:

- ☐ IADigest
- ☐ Research Update
- ☐ Cyber Events Calendar
- ☐ Technical Inquiries Production Report (TIPR)
- ☐ IA Policy Chart Update

Fax completed form to IATAC at 703/984-0773

IATAC
Information Assurance Technology Analysis Center
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171

Calendar

February

NDSS Symposium 2012
5–8 February 2012
San Diego, CA
http://www.isoc.org/isoc/conferences/ndss/12/

CT-RSA 2012
27 February– 2 March 2012
San Francisco, CA
http://ctrsa2012.cs.haifa.ac.il/

March

19th International Workshop on Fast Software Encryption
19–21 March 2012
Washington, DC
http://fse2012.inria.fr/

Pacific Operational Science & Technology Conference
19–22 March 2012
Honolulu, HI
http://www.ndia.org/meetings/2540/Pages/default.aspx

DTIC
26–29 March 2012
Ft. Belvoir, VA
http://www.dtic.mil/dtic/annualconf/2012/DTICConf.html

IANS Mid-Atlantic Information Security Forum
20–21 March 2012
Washington, DC
http://www.iansresearch.com/ians-events

SANS 2012
23–30 March 2012
Orlando, FL
http://www.sans.org/sans-2012/

TechNet Land Forces-Southwest
27–29 March 2012
Tucson, AZ
http://www.afcea.org/events/

April

InfoSec World Conference & Expo 2012
2–4 April 2012
Orlando, FL
http://www.misti.com/default.asp?Page=65&ProductID=5539&ISS=21737&SID=625900

WiSec '12
16–18 April 2012
Tucson, AZ
http://www.sigsac.org/wisec/WiSec2012/

13th Annual Science & Engineering Technology Conference/DoD Tech Expo
17–19 April 2012
Charleston, SC
http://www.ndia.org/meetings/2720/Pages/default.aspx

SANS AppSec 2012
24 April–2 May 2012
Las Vegas, NV
http://www.sans.org/appsec-2012/

May

Joint Warfighting Conference 2012
15–17 May 2012
Virginia Beach, VA
http://www.afcea.org/events/jwc/11/intro.asp

IEEE Symposium on Security and Privacy
20–23 May 2012
San Francisco, CA
http://www.ieee-security.org/TC/SP2012/index.html